**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені ІГОРЯ СІКОРСЬКОГО»**
**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**
Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____2018 р.

# Магістерська дисертація

**на здобуття ступеня магістра**

зі спеціальності: 125 Кібербезпека

на тему: Системи відеоспостереження з використанням комп’ютерного зору в завданнях інформаційної безпеки

Виконав (-ла): студент (-ка) 2 курсу, групи ФБ-71мп
(шифр групи)

Хіміч Андрій Віталійович
(прізвище, ім’я, по батькові)

Науковий керівник к.т.н., доц. Стьопочкіна Ірина Валеріївна_ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.т.н., доцент ФІОТ Жданова О.Г. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені ІГОРЯ СІКОРСЬКОГО»**
**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 125 Кібербезпека («Системи і технології кібербезпеки)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)

«___»_____2018 р.

**ЗАВДАННЯ**
**на магістерську дисертацію студенту**

Хімічу Андрію Віталійовичу

1. Тема дисертації: Системи відеоспостереження з використанням комп'ютерного зору в завданнях інформаційної безпеки
науковий керівник дисертації к.т.н., доц. Стьопочкіна Ірина Валеріївна,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «15» листопада 2018 р. № 4171-с

2. Термін подання студентом дисертації 12.12.2018 р.

3. Об'єкт дослідження _____
_____

4. Вихідні дані _____
_____
_____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____
_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу _____
_____
_____

7. Орієнтовний перелік публікацій _____
_____

8. Консультанти розділів дисертації*

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |
| | | | |
| | | | |

9. Дата видачі завдання _____

Календарний план

| № з/п | Назва етапів виконання магістерської дисертації | Термін виконання етапів магістерської дисертації | Примітка |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Студент _____ (підпис) _____ (ініціали, прізвище)

Науковий керівник дисертації _____ (підпис) _____ (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

# РЕФЕРАТ

Магістерська дипломна робота складається із переліку умовних позначень, вступу, чотирьох розділів, висновків і переліку джерел посилання. Основний зміст складає 84 сторінки друкованого тексту, містить 29 рисунків і 19 таблиць.

Список використаних джерел містить 27 найменувань.

**Мета і завдання дослідження**. Дослідити особливості та перспективи використання систем відеоспостереження з використанням комп'ютерного зору для підвищення рівня фізичного захисту інформації в межах захищеного периметра шляхом організації спостереження за переміщеннями осіб.

**Наукова новизна одержаних результатів**. Результати роботи пропонують альтернативний спосіб використання камер відеоспостереження, що базуються на штучному інтелекті, як доповнюючому способі контролю персоналу для підвищення рівня захисту системи від витоку інформації по фізичним каналам.

**Практичне значення одержаних результатів**. З розвитком області штучного інтелекту та контекстного аналізу зображень, результати даної роботи можуть бути використані у подальших дослідженнях по впровадженню більш складних систем, наприклад в аналізі підозрілої поведінки з точки зору інформаційної безпеки.

**Ключові слова**: системи відеоспостереження, комп'ютерний зір, інформаційна безпека, згорткові нейронні мережі, алгоритм Deep SORT.

## ABSTRACT

Master's thesis consists of a list of symbols, an introduction, four sections, conclusions and a list of sources of reference. The main content is 84 pages of printed text, containing 29 figures and 19 tables.

List of references contains 27 items.

**The purpose and tasks of the study**. To study the peculiarities and prospects of using computer vision-based CCTV systems for increasing the physical protection level of information within the protected perimeter by tracking the motion of people.

**Scientific novelty of the obtained results.** The results of the work suggest an alternative way of using artificial intelligence-based video surveillance cameras as a complement to the method of access control to increase the level of protection of the system from the leakage of information through physical channels.

**The practical value of the obtained results.** With the development of the field of artificial intelligence and context analysis of images, the results of this work can be used in further studies on the implementation of more complex systems, for example, in the analysis of suspicious behavior in terms of information security.


**Keywords**: VIDEO SURVEILLANCE SYSTEMS, COMPUTER VISION, INFORMATION SECURITY, CONVOLUTIONAL NEURAL NETWORKS, DEEP SORT ALGORITHM.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ЗІ – захист інформації

КСЗІ – комплексна система захисту інформації

CNN (англ. Convolutional Neuron Network) – клас глибинних штучних нейронних мереж прямого поширення, який успішно застосовувався до аналізу візуальних зображень.

Deep SORT – Deep Simple Online and Realtime Tracking algorithm

Python - інтерпретована об'єктно-орієнтована мова програмування високого рівня зі строгою динамічною типізацією.

TensorFlow – відкрита програмна бібліотека для машинного навчання цілій низці задач, розроблена компанією Google для задоволення її потреб у системах, здатних будувати та тренувати нейронні мережі для виявлення та розшифровування образів та кореляцій, аналогічно до навчання й розуміння, які застосовують люди.

UML (англ. Unified Modeling Language) - загальнонаціональна мова розробки та моделювання в галузі програмного забезпечення, яка призначена для забезпечення стандартного способу візуалізації дизайну системи.

# ВСТУП

**Актуальність роботи**. Системи відеоспостереження, що використовують штучний інтелект, на сьогоднішній день активно розвиваються та з успіхом починають застосовуватись на масштабному рівні. Покращується як наукова база штучних нейронних мереж, так і обчислювальні потужності технічного обладнання. Результати даного дослідження пропонують новий погляд на використання системи відеоспостереження з комп'ютерним зором, а саме, для підвищення фізичного рівня захисту інформації.

**Мета і завдання дослідження**. Дослідити особливості та перспективи використання систем відеоспостереження з використанням комп'ютерного зору для підвищення рівня фізичного захисту інформації в межах захищеного периметра шляхом організації спостереження за переміщеннями осіб.

**Об'єкт дослідження**. Системи відеоспостереження та реєстрації інцидентів.

**Предмет дослідження**. Методи штучного інтелекту в реалізації обробки даних, одержаних від систем відеоспостереження та реєстрації інцидентів, в завданнях кібербезпеки.

**Задачі дослідження**:

1) Дослідження здобутків в області комп'ютерного зору та огляд існуючих методів рішення.
2) Аналіз алгоритмів та підходів для забезпечення необхідного рівня надійності одержаної системи.
3) Визначення особливостей використання систем розпізнавання образів у камерах відеоспостереження в задачах інформаційної безпеки.
4) Аналіз можливості використання камер відеоспостереження, що базуються на штучному інтелекті, у доповненні з іншими організаційно-технічними методами забезпечення захисту інформації.

5) Побудова архітектури системи розпізнавання образів.
6) Реалізація програмних модулів для функціонування інтелектуальних методів аналізу зображень в складі системи відеоспостереження.
7) Тестування програмних рішень на наборі відеоматеріалів.

**Наукова новизна одержаних результатів**. Результати роботи пропонують альтернативний спосіб використання камер відеоспостереження, що базуються на штучному інтелекті, як доповнюючому способі контролю персонала для підвищення рівня захисту ІС.

**Практичне значення одержаних результатів**. З розвитком області штучного інтелекту та контекстного аналізу зображень, результати даної роботи можуть бути використані у подальших дослідженнях по впровадженню більш складних систем, наприклад в аналізі підозрілої поведінки.

# 1 ОСНОВНІ ЗАСАДИ ВИКОРИСТАННЯ КОМП'ЮТЕРНОГО ЗОРУ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

## 1.1 Опис предметної області

Зорова система людини без проблем здатна до сприйняття оточуючого її світу. Наприклад, вона здатна відокремити головний об'єкт від його оточення, врахувати тонкі закономірності затінення (Рисунок 1.1).

Рисунок 1.1 – Зорова система людини без проблем виділяє об'єкт з навколишнього фону

Також, дивлячись на фото групи людей (Рисунок 1.2), можна без проблем порахувати точну кількість учасників і навіть зробити припущення про їх настрій та стан, основуючись на виразах обличь. Психологи, що вивчають процеси сприйняття, проводять десятиліття, намагаючись зрозуміти, як функціонує візуальна система, і хоча вони можуть використовувати певні оптичні ілюзії для виявлення деяких фундаментальних принципів, остаточних відповідей на всі поставлені запитання на даний момент немає.

Рисунок 1.2 – Приклад застосування комп'ютерного зору у розпізнаванні обличь

Дослідники комп'ютерного бачення розвивали паралельно математичні методи для розпізнавання та відновлення тривимірної форми об'єктів у зображенні. На сьогоднішній день існують доволі надійні методи для точного обчислення часткової 3D-моделі середовища за допомогою тисяч частково перекриваючихся фотографій. З використанням доволі великого набору даних, можливо створювати точні, щільні моделі 3D-поверхні, використовуючи стереопідсилення (Рисунок 1.3).

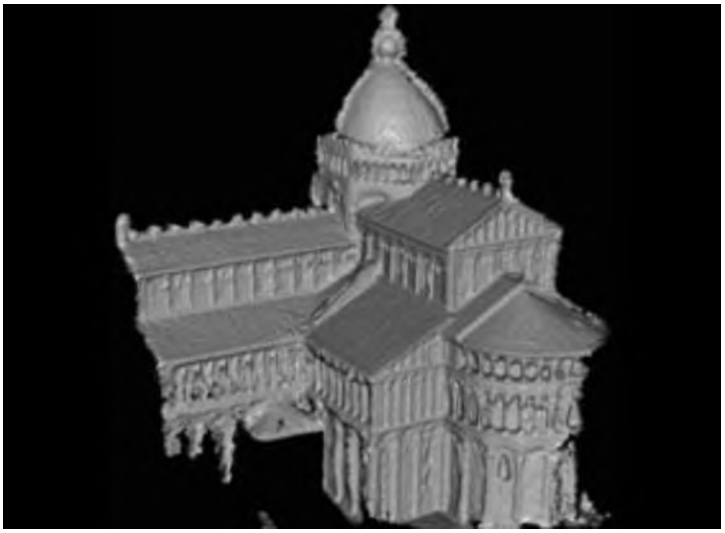

Рисунок 1.3 – Стереосистемні алгоритми зіставлення можуть створювати детальну 3D-модель фасаду будівлі

Сучасні алгоритми відслідковування руху здатні відстежувати переміщення людини, або навіть, групи людей, при доволі складних умовах зйомки (Рисунок 1.4).

Рисунок 1.4 – Приклад роботи алгоритму відстеження людини, що рухається

Однак, незважаючи на дані досягнення, рівень розпізнавання образів та виділення контексту з зображення все ще залишається на доволі низькому рівні, не дотягуючи до рівня дитини дошкільного віку. Причина, через яку

розпізнавання образів є такою складною задачею є те, що сама проблема має зворотню природу, в якій необхідно відновити деякі невідомі дані на основі недостатньої інформації. Тому, необхідно вдаватися до фізичних та імовірнісних моделей, щоб уникнути розбіжностей між потенційними рішеннями. Проте моделювання візуального світу в реальному часі з усіма його особливостями є неможливою задачею на даний момент.

У задачах комп'ютерного зору здійснюються спроби зворотного відновлення прихованої інформації [3], тобто описати світ, що представлений в одному або серії зображень і відтворити його властивості, такі як форма, освітленість та переходи кольору. Люди, які не працювали у цій галузі, часто недооцінюють труднощі проблеми. Це неправильне розуміння того, що бачення повинно бути легким датується ранніми днями штучного інтелекту, коли спочатку вважалося, що пізнавальні (логічні докази та планування) частини інтелекту були по суті складнішими, ніж перцептивні компоненти.

Комп'ютерне бачення сьогодні використовується у різних галузях, які включають:

- Розпізнавання обличь – для покращення фокусування камери, а також для більш релевантного пошуку зображень
- Візуальна аутентифікація – тобто перевірка особистості на основі певних рис обличчя.
- Відслідковування руху транспорту – допоміжний метод контролю дорожнього трафіку та розпізнавання автомобільних номерів.
- Оптичне розпізнавання символів – зчитування рукописних поштових кодів на листах та автоматичне розпізнавання номерного знаку.
- Технічна інспекція – перевірка деталей для забезпечення якості, використовуючи стерео бачення з спеціалізованим освітленням для

вимірювання деформацій крил літальних апаратів або пошук дефектів сталевих деталей з використанням рентгенівського зору.

- 3D-моделювання – повністю автоматизована побудова 3D-моделей з аерофотознімків
- Автомобільна безпека – виявлення непередбачених перешкод, таких як пішоходи на вулиці, в умовах, коли активні методи зору, такі як радар, не працюють
- Об'єднання комп'ютерних зображень (CGI) з реальними відеозаписами

## 1.2 Штучні нейронні мережі та глибоке навчання

Штучна нейронна мережа містить в собі набір взаємопов'язаних пристроїв обробки даних [3]. Дано вхідні значення $w_0, x_1, \dots, x_D$ , де $w_0$ являє собою зовнішній вхід, а $x_1, \dots, x_D$ – входи, з інших блоків обробки (в межах мережі). Пристрій обробки обчислює його вихід як $y = f(z)$. Тут $f$ – передавальна функція, а $z$ отримується шляхом застосування правила розповсюдження, яке відображає всі входи на вхід до $z$. Ця модель єдиного пристрою обробки включає визначення нейрона, де замість правила поширення використовується суматор для обчислення $z$ як зваженої суми всіх вхідних даних.

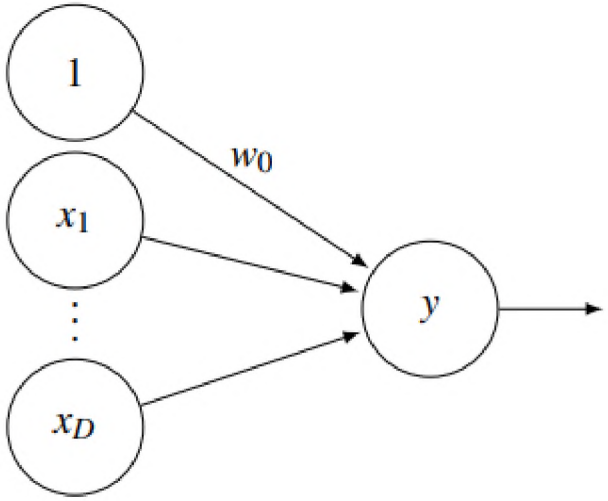


Рисунок 1.5 – Графічне представлення нейронної мережі

Нейронні мережі можуть бути візуально представлені у вигляді спрямованого графа, що називається мережевий граф. Кожен елемент представлена вершиною, позначеною відповідно до виходу, а зв'язок між елементами позначається у вигляді однонапрямлених ребр (Рисунок 1.5).

Для зручності розрізняють вхідні та вихідні елементи. Вхідний елемент обчислює вихід $y := x$, де $x$ – одиничне вхідне значення. Вихідні елементи можуть приймати довільну кількість вхідних значень. В цілому мережа являє собою функцію $y(x)$, розміри якої залежать від кількості вхідних та вихідних елементів, що означає, що вхід мережі приймається вхідними елементами а вихідні елементи формують вихід мережі.

### 1.2.1 Багатошарові перцептрони

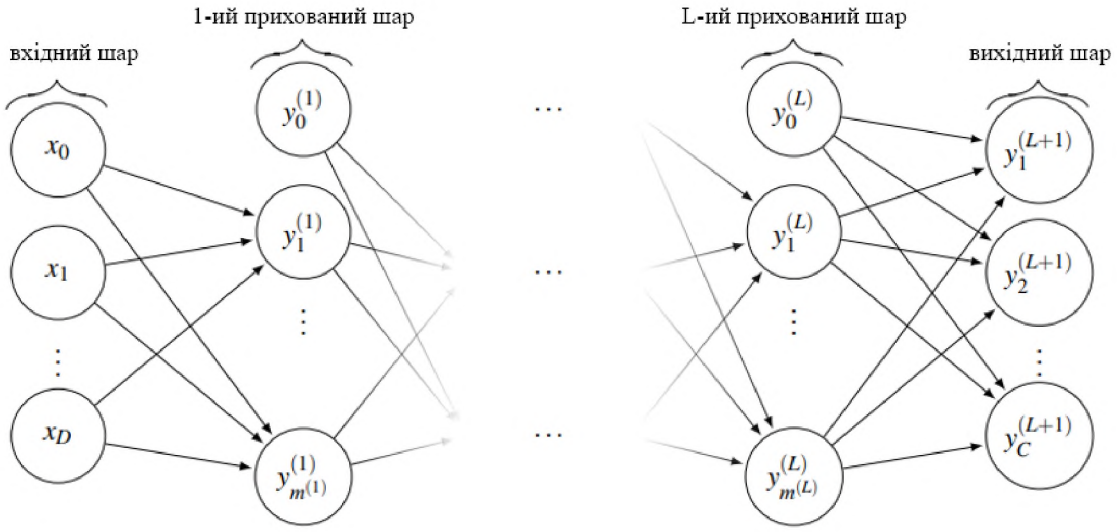


Рисунок 1.6 – Мережевий граф перцептрона з $L+1$ шарами, $D$ входами та $C$ виходами, що містить $I$ прихованих шарів

Перцептрон, що представлений на Рисунок 1.6, має $L+1$ шарів, складається з $D$ входів, $C$ виходів, а також містить $I$ прихованих шарів. Кожний $i$-тий елемент з шару $l$ обчислює вихід:

$$y_i^{(l)} = f(z_i^{(l)}) \text{ , де}$$

$$z_i^{(l)} = \sum_{k=0}^{m^{(l-1)}} w_{i,k}^{(l)} y_{i,k}^{(l-1)} + w_{i,0}^{(l)}$$

де $w_{i,k}^{(l)}$ позначає зважене з'єднання $k$-го елемента у шарі $l-1$ з $i$-тим елементом у шарі $l$, а $w_{i,0}^{(l)}$ являє собою зовнішній вхід до пристрою і називається зміщенням. Тут, $m^{(l)}$ позначає кількість елементів у шарі $l$, так, що $D = m^{(0)}$ та $C = m^{(L+1)}$. Для простоти, зміщення можна розглядати як вагу при введенні фіктивного блоку $y_0^{(l)} := 1$ у кожен з шарів:

$$z_i^{(l)} = \sum_{k=0}^{m^{(l-1)}} w_{i,k}^{(l)} y_{i,k}^{(l-1)}$$

або

$$z^{(l)} = w^{(l)} y^{(l-1)}$$

де $z^{(l)}$, $w^{(l)}$ та $y^{(l-1)}$ позначають відповідні векторні та матричні вигляди про фактичні входи $z_i^{(l)}$, ваги $w_{i,k}^{(l)}$ та виходи $y_{i,k}^{(l-1)}$ відповідно.

У загальному вигляді, функціональне представлення багатошарового перцептрона виглядає наступним чином:

$$y(\cdot, w): \mathbb{R}^D \to \mathbb{R}^C, x \mapsto y(x, w)$$

де вихід вектору $(x, w)$ містить вихідні значення $y_i(x, w) := y_i^{(L+1)}$ та $w$ є вектором усіх вагових коефіцієнтів в мережі.

Нейронна мережа називається глибокою, якщо вона містить більш ніж три прихованих шара. Тренування глибоких нейронних мереж, розглядається як непросте завдання.

### 1.2.2 Передавальна функція

Передавальна функція – залежність вхідного сингала елемента нейронної мережі до вхідного:

$$\mathrm{y} = f(z)$$

Найбільш часто [3] використовуваними типами передавальних функцій є:

- Порогові функції
- Кусково-лінійна функції

– Сигмоїдні функції

У загальному випадку порогова функція визначається як функція Гевісайда (Рисунок 1.7):

$$h(z) = \begin{cases} 1, & \text{якщо } z \geq 0 \\ 0, & \text{якщо } z < 0 \end{cases}$$

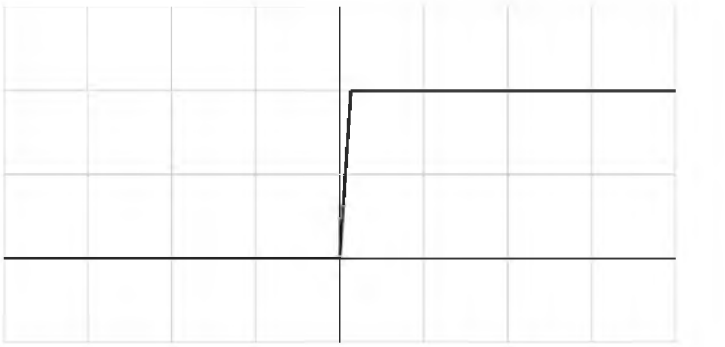

Рисунок 1.7 – Графік функції Гевісайда

Проте як порогові функції, так і кусково-лінійні функції мають деякі недоліки. По-перше, для навчання мережі може знадобитися, щоб функція активації була диференційованою. По-друге, функції нелінійної активації показують кращий результат за рахунок додаткової обчислювальної потужності, яку вони спричиняють (за рахунок нелінійності).

Розповсюдженою передавальною функцією є сигмоїдна функція. Наприклад, логістична сигмоїдна функція (Рисунок 1.8) має вигляд:

$$\sigma(z) = \frac{1}{1 + \exp(-z)}$$

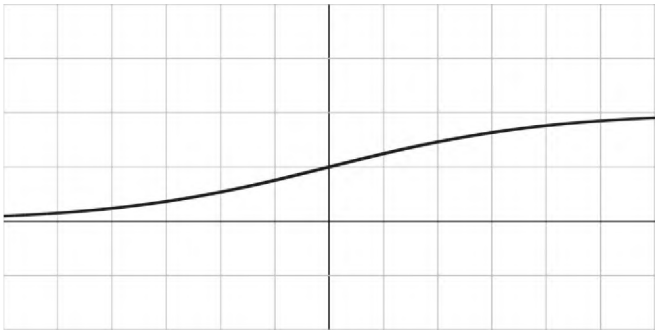

Рисунок 1.8 – Графік логістичної сигмоїдної функції

Графік даної функції має s-подібну форму, а сама функція є диференційованою та монотонною. Функція гіперболічного тангенса $th(z)$ може розглядатися як лінійне перетворення логістичної сигмоїди на інтервал $[-1,1]$. Варто зауважити, що обидві дані передавальні функції є функціями з насиченням (тобто є обмеженими).

При використанні нейронних мереж у задачах класифікації, використовується передавальна функція $softmax$ для елементів виведення, що інтерпретують вихідні значення як апостеріорні ймовірності. В такому випадку виходом $i$-го блоку у вихідному шарі є:

$$\sigma(z^{L+1}, i) = \frac{\exp(z_i^{(L+1)})}{\sum_{k=1}^{C} \exp(z_k^{(L+1)})}$$

Досліди показують, що функція логістичної сигмоїди, а також гіперболічного тангенса, мають погані показники у задачах глибокого навчання [3]. Повідомляється про досягнення найкращих показників за допомогою передавальної функції $sofsign$ (Рисунок 1.9):

$$s(z) = \frac{1}{1 + |z|}$$

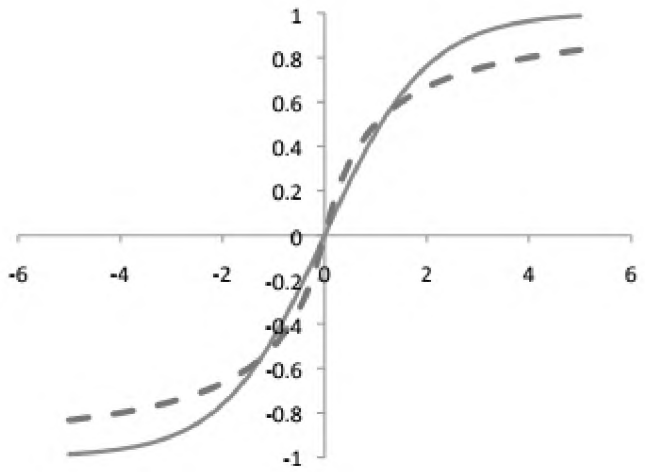


Рисунок 1.9 – Співставлення графіків функцій $th$ (світла лінія)та $sofsign$ (темна пунктирна лінія)

## 1.3 Згорткова нейронна мережа

Згорткові нейронні мережі (CNN – Convolutional Neural Network) є клас глибинних штучних нейронних мереж, який успішно застосовувався до аналізу візуальних зображень [3].

### 1.3.1 Процес згортки

Для простоти представимо зображення, як градації сірого, яке визначається функцією:

$$I: \{1, \dots, n_1\} \times \{1, \dots, n_2\} \to W \subseteq \mathbb{R}, (i, j) \longmapsto I_{i,j}$$

так, що зображення $I$ може бути представлено за допомогою матриці розміром $n_1 \times n_2$. У більшості випадків W представлений набором $\{0, \dots, 255\}$, що

являє собою 8-бітний канал. Тоді кольорове зображення може бути представлено масивом розміру

$n_1 \times n_2 \times 3$ , якщо взяти три кольорові канали, наприклад схему RGB. Виходячи з того, що $K \in \mathbb{R}^{2h_1+1 \times 2h_2+1}$, дискретна згортка зображення $I$ з фільтром $K$ можна представити формулою:

$$(I * K)_{r,s} \coloneqq \sum_{u=-h_1}^{h_1} \sum_{u=-h_2}^{h_2} K_{u,v} I_{r+u,s+v}$$

де фільтр має вигляд:

$$K = \begin{pmatrix} K_{-h_1,-h_2} & \cdots & K_{-h_1,h_2} \\ \vdots & K_{0,0} & \vdots \\ K_{h_1,-h_2} & \cdots & K_{h_1,h_2} \end{pmatrix}$$

Варто зауважити, що поведінка цієї операції на границях зображення повинна бути визначена належним чином. Одним із шляхів вирішення даної проблеми є застосування фільтра лише для тих місць зображення, де він поводить себе коректно. Це, в свою чергу, призводить до того, що вихідний масив буде меншим за початкове зображення.

Розповсюдженим фільтром для згладжування є дискретний фільтр Гауса:

$$(K_{G(\sigma)})_{r,s} = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(\frac{r^2 + s^2}{2\sigma^2}\right)$$

де $\sigma$ є середньо квадратичним відхиленням розподілу Гауса.

### 1.3.2 Згорткові шари

Позначимо згортковий шар як $l$. Тоді вхід на шар $l$ складається з $m_1^{(l-1)}$ відображень ознак, отриманих з попереднього шару, кожне має розмір $m_2^{(l-1)} \times m_3^{(l-1)}$. У випадку, коли $l = 1$, на вхід подається власно необроблене зображення $I$, що складається з одного чи більше складових каналів. Вихід згорткового шару $l$ складається з $m_1^{(l)}$ відображень ознак, що має вигляд матриці розмірності $m_2^{(l)} \times m_3^{(l)}$. Кожна $i$-та матриця відображення ознак $Y_i^{(l)}$ з шару $l$ має наступний вигляд:

$$Y_i^{(l)} = B_i^{(l)} + \sum_{j=1}^{m_1^{(l-1)}} K_{i,j}^{(l)} * Y_j^{(l-1)}$$

де $B_i^{(l)}$ є матрицею зсуву (англ. – bias matrix), а $K_{i,j}^{(l)}$ є фільтром розміру $2h_1^{(l)} + 1 \times 2h_2^{(l)} + 1$, що поєднує $j$-те відображення ознак у шарі $(l-1)$ з $i$-тим відображенням з шару $l$ (Рисунок 1.10). При цьому $m_1^{(l)}$ та $m_2^{(l)}$ знаходяться під впливом ефекту границі, а отже, при використанні дискретної згортки у так званій коректній області, розмір вихідного відображення буде наступним:

$$m_2^{(l)} = m_2^{(l-1)} - 2h_1^{(l)} \text{ та } m_3^{(l)} = m_3^{(l-1)} - 2\mathrm{h}_2^{(l)}.$$

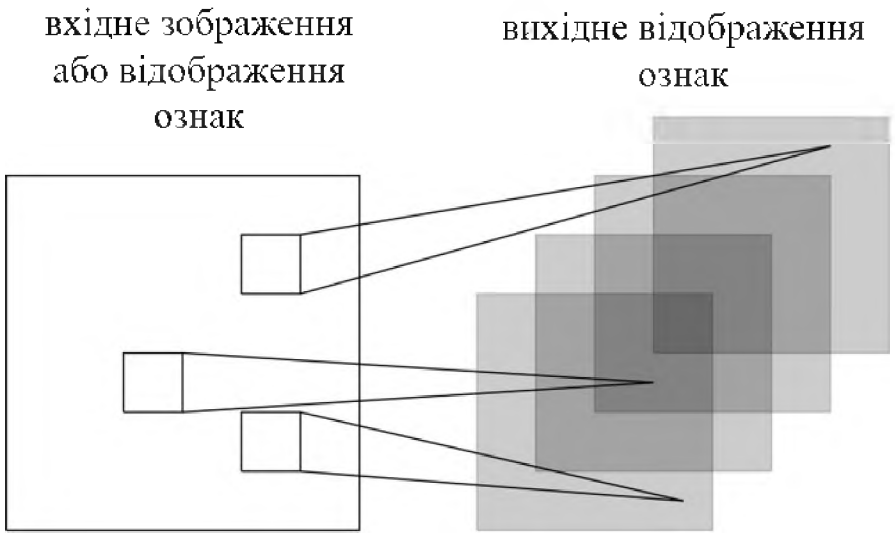


Рисунок 1.10 – Ілюстрація одного зі згорткових шарів. На вхід подається вхідне зображення (у випадку $l = 1$) чи відображення ознак з попереднього шару, що згортається за допомогою набору фільтрів для отримання вихідного відображення.

Часто фільтри, що використовують для обчислення певного відображення ознак $Y_i^{(l)}$, є однаковими, тобто $K_{i,j}^{(l)} = K_{j,k}^{(l)}$, для $j \neq k$. Окрім цього, сума $\sum_{j=1}^{m_1^{(l-1)}} K_{i,j}^{(l)} * Y_j^{(l-1)}$ може вийти за межі підмножини вхідних відображень ознак.

Для того, щоб співвіднести згортковий шар та його операції, з багатошаровим перцептроном, необхідно переписати рівняння:

$$Y_i^{(l)} = B_i^{(l)} + \sum_{j=1}^{m_1^{(l-1)}} K_{i,j}^{(l)} * Y_j^{(l-1)}$$

Кожне відображення ознак $Y_i^{(l)}$ у шарі $l$ складається з $m_1^{(l)} \cdot m_3^{(l)}$ елементів, що розташовані у двовимірному масиві. При цьому елемент в положенні $(r, s)$ обчислює вихід наступним чином:

$$\left(Y_i^{(l)}\right)_{r,s} = \left(B_i^{(l)}\right)_{r,s} + \sum_{j=1}^{m_1^{(l-1)}} \left(K_{i,j}^{(l)} * Y_j^{(l-1)}\right)_{r,s}$$

$$\left(Y_i^{(l)}\right)_{r,s} = \left(B_i^{(l)}\right)_{r,s} + \sum_{j=1}^{m_1^{(l-1)}} \sum_{u=-h_1^{(l)}}^{h_1^{(l)}} \sum_{v=-h_2^{(l)}}^{h_2^{(l)}} (K_{i,j}^{(l)})_{u,v} (Y_j^{(l-1)})_{r+u,s+v}$$

Тренувальні вагові коефіцієнти знаходяться у фільтрах $K_{i,j}^{(l)}$ та матриці зміщень $B_i^{(l)}$.

Також варто зауважити використання процесу відбору виборки (англ. subsampling) для зменшення впливу шумів та спотворень. Це може бути зроблено за рахунок так званих факторів пропуску (англ. skipping factors) $s_1^{(l)}$ та $s_2^{(l)}$. Підхід заключається у пропусканні певної кількості пікселів зображення у горизонтальному та вертикальному напрямах перед повторним приміненням фільтру. При цьому розміри вихідного відображення ознак будуть наступними:

$$m_2^{(l)} = \frac{m_2^{(l-1)} - 2h_1^{(l)}}{s_1^{(l)} + 1} \text{ та } m_3^{(l)} = \frac{m_3^{(l-1)} - 2h_2^{(l)}}{s_2^{(l)} + 1}$$

## 1.4 Фільтр Калмана

Фільтр Калмана давно вважається оптимальним рішенням для багатьох задач відстеження та прогнозування даних [8].

Багато сигналів можна описати наступним чином:

$$y_k = a_k x_k + n_k$$

де $y_k$ – залежний від часу сигнал, $a_k$ - це коефіцієнт посилення, $x_k$ - сигнал, що переносить інформацію і $n_k$ - адитивний шум.

Мета - оцінити $x_k$. Похибкою вважається різниця між очікуваним $\hat{x}_k$ та реальним $x_k$:

$$f(e_k) = f(x_k - \hat{x}_k)$$

Особлива форма $f(e_k)$ залежить від застосування, однак відомо, що ця функція повинна бути позитивною та при цьому монотонно зростати. Функція помилки, яка має ці характеристики являє собою квадрат функції помилки.

Оскільки необхідно враховувати здатність фільтра прогнозувати багато даних протягом певного періоду часу, необхідно ввести більш значущу метрику, а саме очікуване значення функції помилки;

$$f_{\text{втрати}} = E(f(e_k))$$

З цього випливає функція середнього квадратичного відхилення.

$$\epsilon(t) = E(e_k^2)$$

Більш строге виведення може бути виконане з використанням статистики максимальної вірогідності. Це досягається переоцінкою мети фільтра на визначення значення $\hat{x}$ такого, що максимізує вірогідність $y$ . А саме,

$$max[P(y|\hat{x})]$$

Якщо припустити, що адитивний випадковий шум є розподіленим гауссовим шумом зі стандартним відхиленням k, то

$$P(y|\hat{x}) = K_k exp - (\frac{(y_k - a_k x_k)^2}{2\sigma_k^2})$$

де $K_k$ - константа нормалізації. Тоді максимальна функція правдоподібності є наступною:

$$P(y|\hat{x}) = \prod_k K_k exp - (\frac{(y_k - a_k x_k)^2}{2\sigma_k^2})$$

З цього випливає, що

$$\log P(y|\hat{x}) = -\frac{1}{2}\sum_{\text{л}}\left(\frac{\left(y_k - a_k x_k\right)^2}{2\sigma_k^2}\right) + \text{C}$$

Керуюча функція являє собою середньо квадратичне відхилення і може бути максимізована зміною $x_k$. Тому вона застосовується у разі очікуваного відхилення $y_k$ , як гауссового розподілу. У такому випадку середньо квадратичне відхилення служить для забезпечення значення $x_k$, яке максимізує вірогідність сигналу $y_k$.

У даному випадку оптимальний фільтр визначається як той, з набору всіх можливих, що мінімізує середньо квадратичне відхилення.

Припустимо, що ми хочемо знати значення змінної в процесі з формою

$$x_{k+1} = \Phi x_k + \omega_k$$

де $x_k$ - вектор станів процесу в момент часу k (розмірність $n \times 1$); Ф - це матриця (розмірність $n \times m$) переходу станів в процесі від стану у момент часу k до стану у момент часу k + 1, що вважається стаціонарною з плином часу; $\omega_k$ – пов'язаний з процесом білий шум з відомою коваріацією (розмірність $n \times 1$).

Спостереження за цією змінною можна показати у формі

$$z_k = Hx_k + v_k$$

де $z_k$ - фактичне вимірювання величини $x$ у момент часу $k$ (розмірність $m \times 1$); $H$ - це зв'язок, без шуму, між вектором стану та вектором вимірювання, що припускається стаціонарним з плином часу (розмірність $m \times n$); $v_k$ – пов'язана з цим помилка вимірювання, тобто білий шум, що пов'язаний з вимірювання, що має відому коваріацію та нульову перехресну кореляцію з власне шумом процесу (розмірність $m \times 1$).

Як було показано, для мінімізації середньо квадратичного відхилення, для отримання оптимального фільтру можна правильно моделювати системні похибки за допомогою гауссових розподілів. Коваріації двох шумових моделей вважаються стаціонарними з плином часу і виглядають наступним чином

$$Q = E[\omega_k \omega_k^T]$$

$$R = E[v_k v_k^T]$$

З функції середнього квадратичного відхилення, випливає:

$$E[e_k e_k^T] = P_k$$

де $P_k$- матриця коваріації похибки в момент часу $k$ (розмірність $n \times n$).

Рівняння може бути розширене наступним чином:

$$P_k = E[e_k e_k^T] = E[(x_k - \hat{x}_k)(x_k - \hat{x}_k)^T]$$

Приймаючи попередню оцінку $\hat{x}_k$ за $\hat{x}'_k$, що була отримана зі знання системи, можна отримати рівняння для нової оцінки, поєднавши попередню оцінку з даними вимірювань

$$\hat{x}_k = \hat{x}'_k + K_k(z_k - H\hat{x}'_k)$$

де $K_k$ – передавальний коефіцієнт Калмана. В свою чергу, $z_k - H\hat{x}'_k$ - нововведення (відхилення) вимірювання

$$i_k = z_k - H\hat{x}'_k$$

За допомогою підстановок отримаємо

$$\hat{x}_k = \hat{x}'_k + K_k(H\hat{x}_k + v_k - H\hat{x}'_k)$$

$$P_k = E\left[[(I - K_k H)(x_k - \hat{x}'_k) - K_k v_k][(I - K_k H)(x_k - \hat{x}'_k) - K_k v_k]^T\right]$$

Варто зауважити, що, що $x_k - \hat{x}'_k$ є похибкою попередньою оцінки. Вона не корелює з похибкою вимірювання, отже рівняння може бути перезаписаним у вигляді

$$P_k = (I - K_k H)E[(x_k - \hat{x}'_k)(x_k - \hat{x}'_k)^T](I - K_k H) + K_k E[v_k v_k^T]K_k^T$$

Після підстановки маємо

$$P_k = (I - K_k H)P'_k(I - K_k H)^T + K_k R K_k^T$$

де $P'_k$ є попередньою оцінкою $P_k$.

Отримане рівняння є коваріацією оновленої оцінки. Діагональ матриці коваріації містить середні квадратичні відхилення

$$P_{kk} = \begin{bmatrix} E[e_{k-1}e_{k-1}^T] & E[e_k e_{k-1}^T] & E[e_{k+1}e_{k-1}^T] \\ E[e_{k-1}e_k^T] & E[e_k e_k^T] & E[e_{k+1}e_k^T] \\ E[e_{k-1}e_{k+1}^T] & E[e_k e_{k+1}^T] & E[e_{k+1}e_{k+1}^T] \end{bmatrix}$$

Сума елементів діагоналі матриці є слідом матриці. У випадку матриці коваріації похибок, слідом буде сума середньо квадратичних відхилень. Тому дане відхилення можна мінімізувати за допомогою мінімізації сліду $P_k$, що призведе до зменшення сліду $P_{kk}$.

Слід $P_k$ є першою похідною по $K_k$ і результат прирівнюється до нуля для знаходження умови мінімуму.

$$P_k = P'_k - K_k H P'_k - P'_k H^T K_k^T + K_k(H P'_k H^T + R)K_k^T$$

Варто зауважити, що слід матриці дорівнює сліду її транспозиції, отже можемо записати рівняння як

$$T[P_k] = T[P'_k] - 2T[K_k H P'_k] + T[K_k(H P'_k H^T + R)K_k^T]$$

де $T[P_k]$ – слід матриці $P_k$.

Після диференціювання по $K_k$ отримуємо

$$\frac{dT[P_k]}{dK_k} = -2(HP'_k)^T + 2K_k(HP'_kH^T + R)$$

Після прирівнювання з нулем та перестановки доданків

$$(HP'_k)^T = K_k(HP'_kH^T + R)$$

Знаходимо коефіцієнт Калмана $K_k$

$$K_k = HP'_kH^T + R$$

Після остаточної підстановки отримуємо

$$P_k = P'_k - P'_kH^T(HP'_kH^T + R)^{-1}HP'_k$$

$$P_k = P'_k - K_kHP'_k$$

$$P_k = (I - K_kH)P'_k$$

Отримане рівняння - це оновлена матриця коваріації похибок з оптимальним передавальним коефіцієнтом (формула коваріації апостеріорної похибки). Отримані рівняння використовують для оцінки значення $x_k$. Проекція стану досягається за рахунок

$$\hat{x}'_{k+1} = \Phi\hat{x}_k$$

Для завершення рекурсії необхідно знайти рівняння, що проектує матрицю коваріації похибок у наступний інтервал часу $k+1$. Для початку сформуємо вираз для попередньої похибки

$$e'_{k+1} = x_{k+1} - \hat{x}'_{k+1}$$

$$e'_{k+1} = (\Phi x_k + \omega_k) - \Phi\hat{x}'_k$$

$$e'_{k+1} = \Phi e_k + \omega_k$$

Продовжуючи рівняння для $k+1$

$$P'_{k+1} = E[e'_{k+1}e^{T\prime}_{k+1}] = E[(\Phi e_k + \omega_k)(\Phi e_k + \omega_k)^T]$$

Варто зауважити, що $e_k$ та $\omega_k$ мають нульову перехресну кореляцію, оскільки шум $\omega_k$ накопичується у момент часу $\overline{k,\ k+1}$, тоді як $e_k$ – це похибка до моменту $k$.

$$P'_{k+1} = E[e'_{k+1}e^{T\prime}_{k+1}]$$

$$P'_{k+1} = E[\Phi e_k(\Phi e_k)^T] + E[\omega_k {\omega_k}^T]$$

$$P'_{k+1} = \Phi P_k \Phi^T + Q$$

На Рисунок 1.11 представлений остаточний алгоритм фільтру Калмана.


Рисунок 1.11 – Діаграма фільтру Калмана

## 1.5 Угорський алгоритм

Угорський алгоритм — алгоритм комбінаторної оптимізації, що розв'язує задачу про призначення за поліноміальний час $O(n^4)$.

Постановка завдання: Дано $n$ ресурсів, якими необхідно розпорядитись для вирішення $n$ задач, причому на один ресурс має приходитись лише одне завдання. Також, відома вартість вирішення кожної з задач на кожному ресурсі. Необхідно знайти оптимальне призначення завдань ресурсам. У матричному вигляді отримаємо матрицю розмірності $n \times n$, де елемент в $i$-тому рядку та $j$-тому стовпці показує вартість призначення $j$ -тої роботи $i$ -тому ресурсу.

$$C = \begin{bmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{n,1} & \cdots & c_{n,n} \end{bmatrix}$$

Алгоритм [7]:

1. Впорядкувати інформацію в матриці таким чином, щоб рядки матриці представляли «ресурси», а колонки — «завдання», тоді як кожен елемент матриці представляє витрати на виконання певним ресурсом певного завдання.
2. Переконатися в тому, що матриця є квадратною; в протилежному випадку слід додати фіктивний рядок (ресурс) чи колонку (завдання), де кожен елемент буде дорівнювати найбільшому елементу початкової матриці.
3. В кожному рядку від кожного елемента відняти найменше значення для даного рядка.
4. В кожному стовпці від кожного елемента відняти найменше значення для даного стовпця.
5. Викреслити всі нульові елементи з найменш можливою кількістю ліній (якщо кількість ліній дорівнює розмірності матриці, то слід перейти до кроку 9).

6. Додати мінімальний з не викреслених елементів до кожного викресленого елементу (якщо елемент викреслено двома лініями, то додавати слід теж двічі)

7. Від кожного елементу матриці відняти мінімальний елемент.

8. Знову викреслити всі нульові елементи використовуючи найменшу кількість ліній (якщо кількість використаних ліній не дорівнює розмірності матриці, то слід повернутись до кроку 6).

9. Вибрати розподіл «завдань» між «ресурсами» таким чином, щоб в кожному рядкові та стовпці був вибраний лише один нуль.

10. Перенести розподіл на початкову матрицю, ігноруючи фіктивні колонки і рядки. Цей розподіл покаже який «ресурс» яке «завдання» має виконати, а сума виділених елементів покаже загальну вартість виконання робіт.

**Висновки до розділу 1**

Людині та вищим тваринам буквально на кожному кроці доводиться розпізнавати, приймати рішення і вчитися. Наука про штучні нейронні мережі виникла з прагнення зрозуміти, яким чином мозок вирішує такі складні завдання, і реалізувати ці принципи в автоматизованих системах.

Поки штучні нейронні мережі є лише дуже спрощеними аналогами природних нейронних мереж, оскільки нервові системи тварин і людини набагато складніше тих пристроїв, які можна створити за допомогою сучасних технологій. Проте, навіть цього рівня буває достатньо для успішного вирішення багатьох практичних завдань.

До таких завдань, на сьогоднішній день, належать задачі розпізнавання тексту, моніторинг автомобільного трафіку, моделювання 3-D об’єктів на основі набору статичних зображень, а також виявлення та відслідковування переміщень об’єктів.

Саме методи відслідковування об’єктів, а саме людей, на основі відеозаписів починають активно використовувати різноманітні організації державного та приватного секторів. Для державних організацій, мета полягає у забезпеченні громадського порядку, а приватні організації прагнуть забезпечити виробничу безпеку та безпеку бізнесу. Однак у часи зростаючої цінності комерційної таємниці, на даний момент мало уваги приділяється саме безпеці в інформаційному сенсі.

У розділі були досліджені основні терміни та засади розпізнавання образів, які були сформовані за останні пів століття. Також були розглянуті допоміжні алгоритми, такі як фільтр Калмана та Угорський алгоритм, як важливі складові майбутньої системи.

# 2 ОСОБЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ ЯК ЗАСОБУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 2.1 Канали витоку інформації

Витік конфіденційної інформації – це безконтрольний вихід конфіденційної інформації за межі ІС або кола осіб, яким вона була довірена по службі, відома в процесі роботи. Цей витік може бути наслідком;

- розголошення конфіденційної інформації;

- відходу інформації по різним, головним чином технічним, каналам;

- несанкціонованого доступу до конфіденційної інформації різними способами.

Розголошення інформації її власником або іншими власником є навмисні або необережні дії посадових осіб і користувачів, яким відповідні відомості у встановленому порядку були довірені по службі або по роботі, що призвели до ознайомлення з ним осіб, не допущених до цих відомостей.

Можливий безконтрольний відхід конфіденційної інформації з візуально-оптичних, акустичних, електромагнітних і інших каналів.

Несанкціонований доступ – це протиправне навмисне оволодіння конфіденційною інформацією особою, що не має права доступу до охоронюваних відомостей.

У рамках даної роботи акцент ставиться саме на фізичних каналах витоку інформації та фізичному несанкціонованому доступі до захищених інформаційних ресурсів:

– Викрадення/копіювання/знищення фізичних носіїв інформації

– Несанкціонований доступ персоналу та сторонніх осіб до об’єкта
– Перехоплення інформації по акустичним/візуальним каналам витоку (підслуховування, підглядання)

## 2.2 Автоматизовані системи відеоспостереження у задачах розпізнавання аномальної поведінки

Автоматизовані системи відеоспостереження складаються з мережі відео-датчиків, що проводять спостереження за людьми, при цьому враховуючи їх поведінкові характеристики та виділяють серед них ті, що можуть становити небезпеку. Даний підхід знаходить застосування в системах, де існують певні універсальні явні (візуальні) метрики, що дозволяють стверджувати про стан безпеки/небезпеки.

Прикладом даних метрик може бути детектування певних об’єктів, що свідчать про небезпеку, як наприклад зброю (Рисунок 2.1).

Рисунок 2.1 – Розпізнавання збройного нападу

Іншою аномалією, що може бути свідченням незвичності подій, що відбуваються, є поза людини та швидкість руху (Рисунок 2.2).

Рисунок 2.2 – Розпізнавання незвичної поведінки

Системи комп’ютерного зору, що натреновані на розпізнавання людського руху, будуть вважати рух інших транспортних засобів, наприклад велосипеду (Рисунок 2.3), аномальним, та сповіщати про це оператора.

Рисунок 2.3 – Аномальний рухаючийся об'єкт (велосипедист)

Однак, в галузі інформаційної безпеки є проблематичним сам факт того, що критерії інформаційної безпеки є більш складними. Наприклад, фізичний доступ до певного об'єкта інформаційної безпеки з боку однієї особи є нормою, в той час як та ж сама дія зі сторони іншої особи може бути порушенням рівню доступу. Більш того, більш менш надійне виявлення самого факту фізичного доступу до певного інформаційного ресурсу є складною задачею.

## 2.3 Модель взаємодії людини і об'єкта з точки зору інформаційної безпеки

Можливим рішенням проблеми може виступати модель взаємодії людини з об'єктами (human-object interaction) (Рисунок 2.4). Дана модель була досліджена у роботі.


Рисунок 2.4 – Результат роботи iCAN

У цій роботі вони запропонували модуль, що використовує контекстуальний підхід, а також навчається виділяти інформативні регіони, використовуючи зовнішній вигляд людини або об’єкта. Контекст дає підказки про те, на які регіони в образі необхідно звернути увагу. Наприклад, щоб визначити, чи тримає людина у руці предмет, потрібно звернути увагу на область навколо рук людини. З іншого боку, при наявності велосипеда на зображенні, необхідно приділити увагу позі людини, що знаходиться поруч. Це також допомагає уникнути можливих похибок, оскільки у такому випадку їзда або ведення велосипеда є різними діями. Система також концентрується на очах людини для визначення її центру уваги.

Однак є ряд недоліків, що на даний момент унеможливлюють застосування даного підходу у системах відеоспостереження.

1) Швидкодія. Системи відеоспостереження з використанням алгоритмів розпізнавання образів мають бути достатньо швидкими для одночасного відстеження десятків людей за допомогою кожної з наявних камер. І хоча iCAN дозволяє відслідковувати взаємодію людини і об'єкта у реальному часі з задовільною частотою кадрів, її масштабованість не є достатньою.
2) Ракурс. Система потребує прямого ракурсу для оптимальної роботі. Камери відеоспостереження загалом знаходяться вище рівня людини, що обмежую відстеження зорового центру уваги людини, що є найбільш критичним аспектом фізичного захисту інформаційної системи
3) Аналіз дій людини. Не зважаючи на приголомшуючу точність опису певних ситуацій, iCAN фокусується на процесі дії (наприклад, людина тримає документ), а не на результаті (людина сховала документ у валізу), що не дозволяє на даному етапі аналізувати дії, що потенційно призводять до витоку інформації.

Описаний ряд недоліків частково буде виправлений у майбутньому зростаючими потужностями обчислювальної техніки, і в більшій мірі, подальшими активними дослідженнями в даній галузі.

## 2.4 Використання штучного інтелекту у системах відеоспостереження для підвищення рівня інформаційної безпеки

І хоча, системи розпізнавання образів на даний момент не можуть бути використані для розпізнавання факту фізичної інформаційної загрози. Вони можуть бути використані як допоміжний механізм вже існуючих рішень в завданнях інформаційної безпеки.

Головним завданням камер відеоспостереження є передача візуальної інформації обслуговуючому персоналу про стан зони спостереження. Оскільки об’єкти, що підлягають методам інформаційного захисту, є по своїй суті ізольованими, в більшості випадків, єдиними динамічними об’єктами є люди, що знаходяться на його території. Отже, витягування суті зображення в цьому сенсі буде виявлення факту наявності і положення людей у певній області, обмеженій полем зору камери.

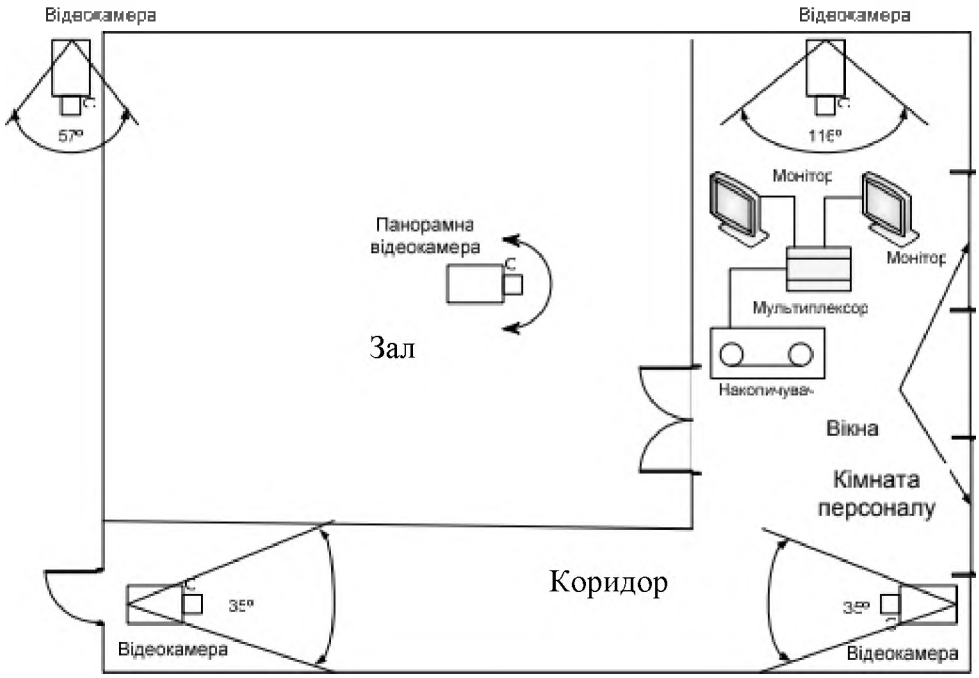


Рисунок 2.5 – Приклад розташування відеокамер на захищеному об'єкті

Комп’ютерний зір дозволяє даний процес визначення описаних ознак. Більш того, такі алгоритми показали свою відносну надійність та швидкодію. Для максимізації результату роботи даного підходу необхідні наступні припущення:

1) Камера є статичною. У більшості випадків це не є проблемою, оскільки при охороні закритих приміщень перевага надається певному напряму (Рисунок 2.5)

2) Дані з камер відеоспостереження зберігаються деякий час на носіях. Даний сценарій є ймовірним, оскільки у захищених об’єктів величина ризику переважує ціну закупівлі і обслуговування носіїв даних.
3) Кількість камер є достатньо великою для поставання питання про термін зберігання даних. У випадку ретроспективи успішного витоку інформації, дані з камер за відповідний період часу можуть бути знищені, що ускладнює розслідування інциденту.
4) Система відеоспостереження є доповненням до певної системи аутентифікації, наприклад смарт-карт (Рисунок 2.6).

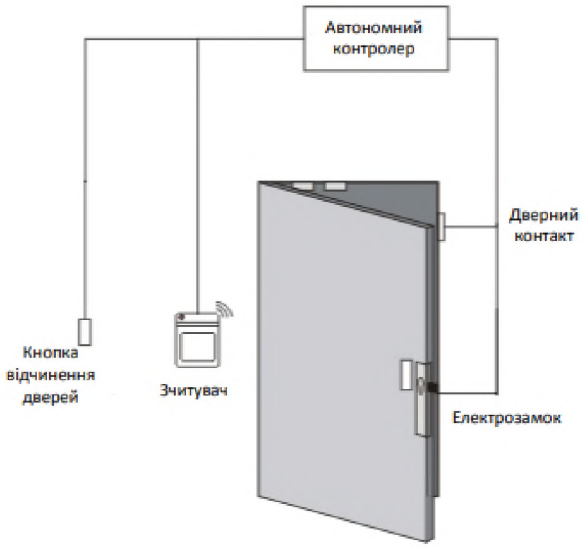


Рисунок 2.6 – Система з використанням смарт-карти

У даній роботі, камери відеоспостереження також розглядаються як об’єкт інформаційної безпеки. У Таблиця 2.1 наведені потреби безпеки та конфіденційності на різних етапах у системі відеоспостереження. Застосування комп’ютерного зору не повинно зашкодити жодному з цих аспектів, інакше сама суть застосування буде втрачена.

Таблиця 2.1 – Вимоги до безпеки та конфіденційності на різних етапах відеоспостереження

| *Компонент безпеки* | | *Запис* | *Передача даних* | *Моніторинг* | *Зберігання даних* |
|---|---|---|---|---|---|
| Приватність | 1. Приватність | Згода<br>Анонімність<br>Властивості запису | Немає | Довіра до оператора<br>Анонімність | Захист від незаконного копіювання |
| Безпека | 2. Конфіденційність | Безпека ПО та інфраструктури | Шифрування даних<br>Безпека приватних ключів | Немає | Шифрування даних<br>Безпека приватних ключів |
| | 3. Цілісність | Безпека ПО та інфраструктури | Відсутність перебоїв сигналу | Актуальність даних | Цілісність |
| | 4. Автентичність | Безпека ПО та інфраструктури | Аутентифікація камери<br>Мітка часу | Мітка часу | Немає |
| | 5. Доступність | Відсутність втрат даних | Немає | Постійний моніторинг | Безпека ПО та інфраструктури |
| | 6. Авторизація | Немає | Немає | Система контролю доступу | Немає |
| | 7.Інші | Безпека ПО та інфраструктури | Немає | Немає | Безпека ПО та інфраструктури<br>Видалення після певного строку |

Для підвищення рівня інформаційної безпеки було запропоновано використання комп'ютерного зору, що виконує функції слідкування за переміщенням людей, та відповідає наступним критеріям:

1) Кожний об'єкт, що відстежується, має унікальний ідентифікатор, який отримується у момент детектування.
2) Система має коректно обробляти тимчасовий вихід об'єкта з полю зору камери, при чому час має бути регульованим.
3) Шанс втрати об'єкта, в результаті якого необхідна його повторна ідентифікація, є мінімальною.
4) Швидкодія дозволить робити обчислення у режимі реального часу та при цьому має прийнятну масштабованість
5) Система не порушує попередні вимоги до безпеки та конфіденційності даних на різних етапах відеоспостереження
6) Система має візуалізувати результати обробки для поліпшення роботи оператора.

У запропонованій системі можна виділити наступні ключові задачі:

1) Отримання ідентифікатора особи при її реєстрації камерами відеоспостереження у давному підході є ключовою проблемою, оскільки його коректність та унікальність сильно впливає на роботу системи в цілому. Найкращим підходом, у цьому випадку, буде служити пункт контролю з використанням певних аутентифікаторів, наприклад зчитувача смарт-карток. Також є можливим використання засобів біометрії, проте ціна готових рішень є вищою, у порівнянні з альтернативами.

2) На території об'єктів, де наявність сторонніх осіб (наприклад тих, перебувають на території об'єкту за гостьовим посвідченням) є невідворотною, а вартість впровадження комплексних мір захисту периметру є необґрунтовано високою, є сенс у виділенні даних сторонніх осіб на моніторі оператора. Для

поліпшення роботи операторів необхідним є виокремлення важливих з точки зору інформаційної безпеки подій. Даний підхід, за умови надійного алгоритму розпізнавання ознак людини та відслідковування переміщень може забезпечити підвищення рівня використання системи відеоспостереження, оскільки постійна увага оператора буде одночасно сконцентрована на меншій кількості об'єктів. Їх переміщенням необхідно приділяти більшу увагу і приймати необхідні міри у разі їх довгострокової відсутності у полі зору засобів спостереження.

3) Також, доступ до даних аутентифікації у описаної системи є обмеженим, з причин конфіденційності та факту того, що програми-аутентифікатори в основному є сторонніми, а отже не мають чітко врегульованої структури. Вирішити це питання можна за рахунок використання API зі сторони запропонованої системи, що дозволяє використання її функціоналу у парі з даними з інших джерел шляхом використання конекторів, написаних під певний набір загальновживаних систем.

4) Для поліпшення стану інформаційної захищеності об'єкту, також було запропоновано використання даних про переміщення осіб, отриманих в результаті роботи алгоритму відстеження, як статистичних. Суть полягає у використанні метрик, що дозволяють стверджувати про потенційні вразливості певних зон захищеного об'єкту на основі наявності у даній зоні людей, що не мають необхідного рівня доступу. Дані про переміщення осіб, будучи по своїй суті, сукупністю координат точки, ідентифікатора особи ти ідентифікатора камери у кожний момент часу, займають менше місця на фізичних носіях інформації, а отже підлягають можливості їх довгострокового накопичення.

5) Забезпечення можливості ручного контролю системи відслідковування переміщень. У разі втрати об'єкта спостереження, оператор повинен мати можливість власноруч вказати системі втрачений об'єкт, що підвищить рівень уваги оператора у довгостроковій перспективі а також компенсує можливі помилки самої системи.

У результаті можна сформувати наступні фактори впливу на рівень інформаційної безпеки, описані у Таблиця 2.2. Окремо варто зауважити пункт 5, оскільки збереження додаткових даних та їх витік може призвести до порушення приватності. В якості рішення даної проблеми пропонується розмежування ідентифікатора особи з камер відеоспостереження та ідентифікатора особи з системи аутентифікації.

Таблиця 2.2 – Фактори впливу на рівень інформаційної безпеки

| *Чинник* | *Фактор впливу* |
|---|---|
| 1) Використання ідентифікатора, отриманого під час допуску особи на територію захищеного об’єкта для відстеження її подальших переміщень. | Підвищення рівня безпеки за рахунок використання додаткових засобів аутентифікації. Рівень впливу визначається ефективністю алгоритму відстеження та власне системи аутентифікації. |
| 2) Виокремлення осіб з фону на відеозаписі, підсвічення з урахуванням певної встановленої легенди, наприклад рівня допуску. | Підвищення рівня контрольованості переміщень осіб, що становлять потенційну загрозу для витоку інформації, проте наявність яких на території об’єкту є неминучою (наприклад, особи, що знаходяться за гостьовим посвідченням). |

Кінець Таблиця 2.2

| *Чинник* | *Фактор впливу* |
|---|---|
| 3) Сповіщення оператора про тимчасову втрату сліду певної особи, що становить потенційну небезпеку (наприклад особи з низьким рівнем допуску) | Покращення спостережності ситуації на території об'єкта за рахунок наголошення уваги оператора на окремому секторі відеоспостереження. Рівень впливу визначається здатністю алгоритму до довгострокового відслідковування особи з низьким шансом її втрати. |
| 4) Сповіщення оператора про остаточну втрату сліду певної особи з можливістю власноруч відновити слід. | Покращення спостережності ситуації на території об'єкта за рахунок наголошення уваги оператора на окремому секторі відеоспостереження. Рівень впливу визначається здатністю алгоритму до довгострокового відслідковування особи з низьким шансом її втрати. |
| 5) Збереження даних про переміщення осіб на території об'єкту у форматі вихідних даних системи комп'ютерного зору для їх подальшого використання у статистичних цілях та при розслідуванні інцидентів | Підвищення рівня захисту за рахунок додаткових записів про стан об'єкту. Можливість використання статистичних даних для виявлення аномалій та закономірностей переміщень для аргументованого внесення змін у вже існуючу КСЗІ. |

Діаграма, що описує процес виконання запропонованих вимог у ході функціонування системи на території захищеного об'єкту, наведена на Рисунок 2.7.


Рисунок 2.7 – Схема роботи системи відеоспостереження з використанням штучного інтелекту

### 2.4.1 Побудова теплових карт переміщень на основі зібраних даних

Як було зазначено, отримані дані можна використовувати у статистичних цілях. Одним із таких методів є отримання так званих теплових карт (англ. – heatmap). Теплова карта являє собою графічне зображення даних, де окремі значення, що містяться в матриці даних, представлені у вигляді відповідних градієнтів кольорів. У цьому випадку в якості даних використовується інформація з камер відеоспостереження про переміщення осіб на території захищеного об'єкта. На Рисунок 2.8 можна бачити приклад використання даної технології. Інтенсивність переміщень позначається більш яскравим кольором (або більш світлим відтінком у випадку чорно-білого зображення). Як можна бачити на даній теплової карті, алгоритм  не розрізняє переміщення окремих людей, оскільки не має задачі до відслідковування переміщень кожної особи.

Рисунок 2.8 – Приклад теплової карти переміщень людей (відтінки сірого позначають частоту проходження)

У випадку, якщо дану технологію впроваджувати, як доповнюючу, у КСЗІ, має сенс виокремлювати переміщення кожної окремої особи. У представлені запропоновані шляхи використання отриманих даних у сенсі підвищення рівня інформаційної безпеки.

Таблиця 2.3 – Шляхи використання теплових карт переміщень персоналу у сенсі КСЗІ

| *Шлях використання* | *Вплив на КСЗІ* |
|---|---|
| Виявлення закономірностей переміщень | – Можливість реорганізації системи відеоспостереження з метою підвищення її продуктивності<br>– Аналіз ефективності використання компонентів контролю доступу, з якими особи напряму взаємодіють<br>– Можливість реорганізації персоналу з метою мінімізації переміщень та взаємодії осіб з різним рівнем доступу<br>– Більш ефективний розподіл витрат на КСЗІ з урахуванням відмінності у рівні та джерелі загроз в залежності від часу. |
| Виявлення аномалій переміщень (окремих осіб відповідно до їх ріння доступу) | – Можливість своєчасно реагувати на потенційно несанкціонований доступ |

## Висновки до розділу 2

У розділі була проаналізована можливість використання камер відеоспостереження, як самостійного методу захисту інформації. Для перелічених у розділі каналів витоку інформації, насьогодні самостійне застосування алгоритмів комп'ютерного зору в камерах в КСЗІ є недостатньо ефективним по причині відсутності як теоретичної бази з розпізнавання аномальної поведінки в термінах фізичного ЗІ, так і недостатньої потужності обчислювальних засобів.

Незважаючи на це, комп'ютерний зір з успіхом може бути використаний як допоміжний засіб для підвищення рівня захисту ІС. При поєднанні з системою аутентифікації, наприклад, смарт-картами, система відеоспостереження зі штучним інтелектом дозволить відслідковувати переміщення людей, при цьому однозначно ідентифікуючи їх, що відкриває можливості для створення нових правил безпеки а також поліпшує роботу операторів.

Сценарій використання представляє собою наступні кроки:

1) Ідентифікація особи камерами відеоспостереження та надання особі ідентифікатора.

2) З використанням засобів аутентифікації, таких як смарт-карта чи біометрія, особистість людини співставляється з ідентифікатором особи, отриманим з камер відеоспостереження. Використання сторонніх засобів для аутентифікації дозволяє налаштувати різні рівні контролю, основуючись на рівні допуску особи, що пройшла аутентицікацію.

3) При переміщенні людини по території захищеного об'єкту, система намагається не втратити її слід, таким чином, зберігаючи ідентифікатор особи незмінним впродовж усього часу перебування.

4) При втраті сліду, система намагатиметься його відновити, виходячи з припущення про незмінну кількість осіб на території об'єкту у короткому

часовому діапазоні. При неможливості відновити слід, система намагається сповістити оператора відеоспостереження та пропонує можливість власноруч виправити помилку.

5) Усі дані про переміщення зберігаються у компактній формі та можуть бути використані для збору статистки переміщення, оскільки без додаткових ідентифікаторів по своїй суті є анонімними. У разі використання додаткових ідентифікаторів, збережені дані можна використовувати як допоміжні засоби у процесі розслідування інцидентів.

У якості основного шляху використання збережених даних про переміщення осіб, було запропоновано побудова теплових карт, що дозволять аргументоване внесення змін у вже існуючу КСЗІ. На основі теплових карт, можна робити висновки про міру ефективності використання інших систем захисту інформації і контролю доступу. Також теплові карти дають можливість до детектування аномальних переміщень конкретних осіб, тобто може виступати у ролі превентивних засобу з виявлення потенційних загроз.

Запропоновані рішення органічно доповнюють вже існуючі засоби із забезпечення безпеки, в тому числі і інформаційної. Описана система не порушує попередні вимоги до безпеки та конфіденційності даних на різних етапах відеоспостереження.

# 3 РЕАЛІЗАЦІЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ, НАЦІЛЕНОЇ НА ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Для вирішення поставленої задачі, був використаний алгоритм Deep SORT (Deep Simple Online and Realtime Tracking algorithm), що використовує бібліотеку машинного навчання Tensorflow. В якості вхідних параметрів для нейронної мережі були використані дані, отримані F. Yu та ін. у своїй роботі [9].

Користуючись швидким розвитком розпізнавання забражень на основі CNN, алгоритм використовує його модифікацію під назвою Faster Region CNN (FrRCNN). FrRCNN являє собою повноцінний фреймворк, що складається з двох етапів. Перший етап витягує особливі ознаки зображення і пропонує регіони для другого етапу, який потім класифікує об'єкт у запропонованому регіоні. Використання даного підходу підвищує модульність рішення, створюючи більш ефективну системи розпізнавання зображень.

## 3.1 Модель оцінки

У даному розділі описано об'єктну модель, тобто представлення і модель руху, що використовується для передачі рис цілі в наступний кадр. Відсутність об'єкта між кадрами розцінюється як його лінійний рівномірний рух, який не залежить від інших об'єктів та руху камери. Стан кожною цілі має наступний вигляд

$$X = [u, v, s, r, \dot{u}, \dot{v}, \dot{s}]^T$$

де $u$ та $v$ представляють горизонтальне та вертикальне положення центрального пікселю цілі, $s$ та $r$ представляють масштаб і відношення сторін прямокутника, що обмежує ціль. Важливо зауважити, що відношення сторін приймається як константне значення. У момент детектування цілі, обмежуючий її прямокутник

використовується для оновлення її стану і положення, в той час як компонент швидкості вирішується за допомогою фільтру Калмана. При відсутності відстежуваної цілі у певний момент часу, її стан оновлюється, виходячи з припущення про рівномірний прямолінійний рух.

## 3.2 Проектування системи

У даному розділі описана структура системи. Загалом, система складається з модулів детектування нових об’єктів, відслідковування попередньо виявлених об’єктів, візуалізатора результатів роботи та головного модуля управління. Структура системи у даному розділі описана мовою UML за допомогою діаграми класів та діаграми компонентів.

Діаграма класів представляє собою схему статичної структури, яка описує структуру системи, показуючи класи системи, їх атрибути, операції (або методи) та взаємозв'язок між об'єктами.

Діаграма пакетів, в свою чергу, відображає залежності між пакетами, що складають модель системи. Пакет в сенсі мови UML є групою елементів системи , що є згрупованими за певної логікою та ділять спільний простір імен.

На Рисунок 3.1 представлений клас, що відповідає за зберігання даних про виявлений об’єкт. Він містить наступні атрибути:

- Коефіцієнт впевненості детектування об’єкту
- Вектор ознак, що описує об'єкт
- Координати прямокутника, що описують виявлений об’єкт.

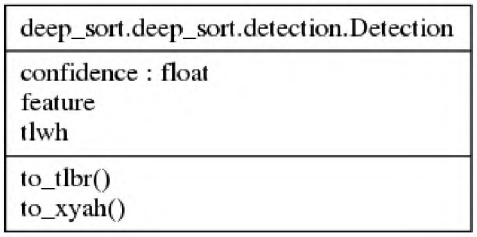


Рисунок 3.1 – Діаграма класів модуля виявлених об'єктів

На Рисунок 3.2 міститься клас, що описує поточний стан об’єкта. Щойно створені сліди класифікуються як «гіпотетичні», доки не знайдено достатніх доказів. Після цього, стан сліду змінюється на «підтверджено». Слід, що був знищений, позначається як «видалений» і є кандидатом на видалення.

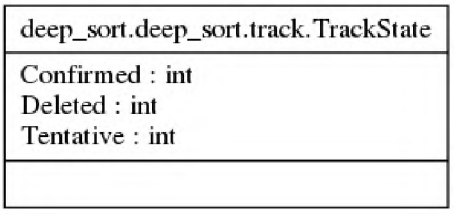


Рисунок 3.2 – Діаграма класів модуля контролю стану сліду цілі

На Рисунок 3.3 представлений клас, що відповідає за збереження даних про слід об’єкта спостереження та містить наступні атрибути:

- Загальна кількість кадрів після першого входження об’єкта у поле зору
- Матриця коваріації початкового розподілу стану
- Набір ознак об’єкта, що оновлюється з кожним новим обчисленням
- Загальна кількість оновлень вимірювань
- Вектор середніх величин розподілу поточний стану
- Поточний стан сліду
- Загальна кількість кадрів після останнього оновлення вимірювань

- Унікальний ідентифікатор сліду, а отже, і самого об’єкта

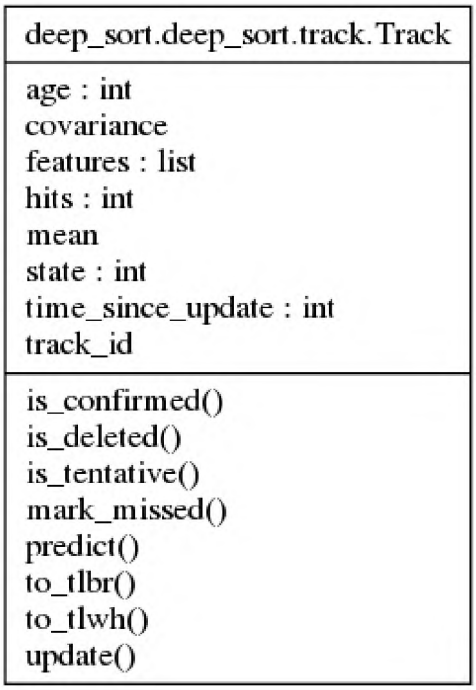


Рисунок 3.3 – Діаграма класів модуля по роботі зі слідами цілі

Модуль, зображений на Рисунок 3.4, відповідає за одночасне відслідковування відразу декількох об’єктів. Складовою частиною модуля є клас, відповідальний за припущення про стан об’єкта на поточний момент часу, що використовує описаний у розділі 1.4 фільтр Калмана. Власне клас обробки слідів містить наступні атрибути:

- Фільтр Калмана для фільтрації цільових траєкторій у просторі зображення
- Максимальна кількість кадрів для втраченого об’єкта, перш ніж його слід буде видалено
- Максимальне значення відношення площі перетину двох прямокутників, що описують об’єкти, до їх об’єднання. Необхідна для коректної обробки перекриття одного об’єкта іншим.
- Кількість кадрів, на яких слід залишається на етапі ініціалізації
- Список активних слідів на поточний момент часу

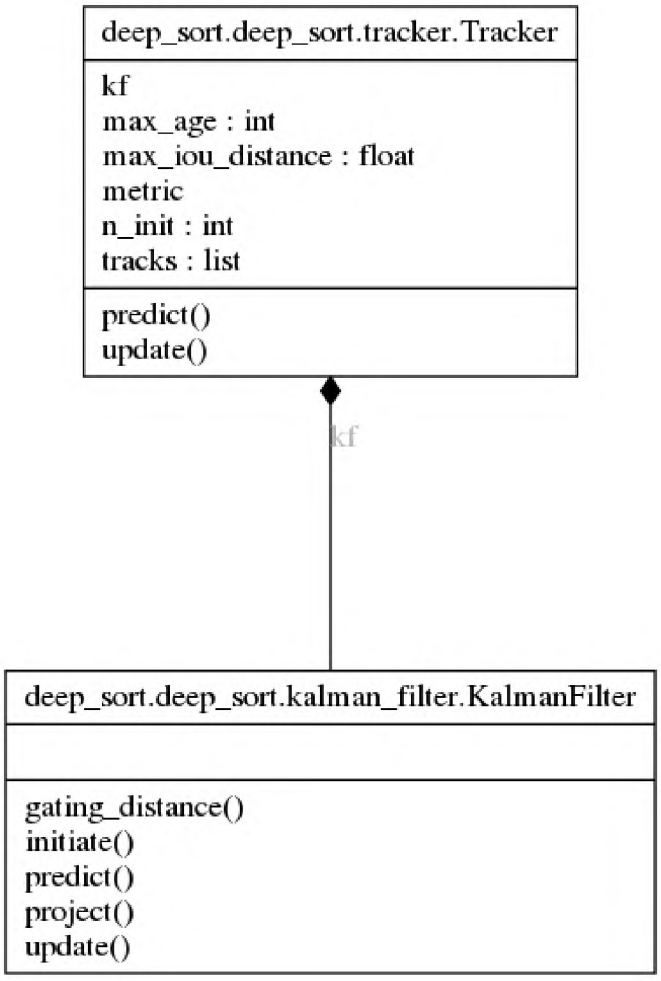


Рисунок 3.4 – Діаграма класів модуля відслідковування декількох об'єктів

Модуль візуалізації (Рисунок 3.5) представлений у вигляді взаємодії двох класів. Він включає в себе атрибути з налаштування відображення результату роботи. До характеристик, які відображаються поверх відеозапису належать прямокутник, що описує об’єкт та має певний колір, в залежності від налаштувань системи, а також унікальний ідентифікатор об’єкта.

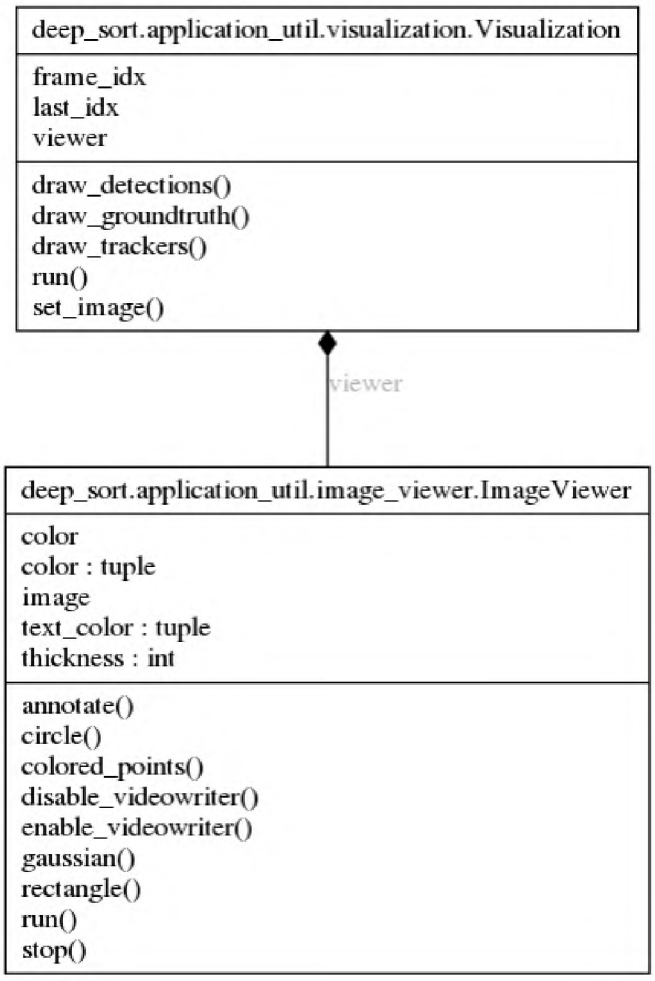


Рисунок 3.5 – Діаграма класів модуля візуалізації виявлення об'єктів

У разі, коли візуалізація результату роботи не є необхідною, існує модуль-заглушка, представлений на Рисунок 3.6.

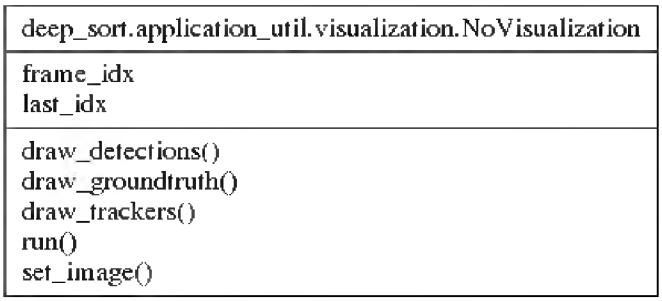


Рисунок 3.6 – Діаграма класів модуля-заглушки візуалізації виявлення об'єктів

Спроектована діаграма пакетів, представлена на Рисунок 3.7, показує взаємозв'язок модулів у системі. З діаграми видно, поєднання основних компонентів системи у головний виконавчий модуль. Для головного виконавчого модулю був спроектований консольний інтерфейс взаємодії. Даний інтерфейс має наступні можливості.

- Зчитування відеопослідовності за вказаним місцезнаходженням
- Запису результату роботи на носій
- Виводу результату роботи на монітор користувача
- Налаштування порогового значення коефіцієнту впевненості, який впливає на чутливість системи до потенційного виявлення нових об'єктів
- Налаштування максимального часу, за який об'єкт вважається втраченим назавжди, а його слід видаляється
- Налаштування максимального коефіцієнту перекриття, після якого об'єкт вважається тимчасово зниклими, а для його подальше місцеположення вираховується тільки за рахунок фільтру Калмана.
- Налаштування мінімальної висоти об'єкта, що дозволяє зменшити кількість похибок першого роду у процесі детектування.

Даний інтерфейс дозволяє гнучке налаштування системи відповідно до умов експлуатації.

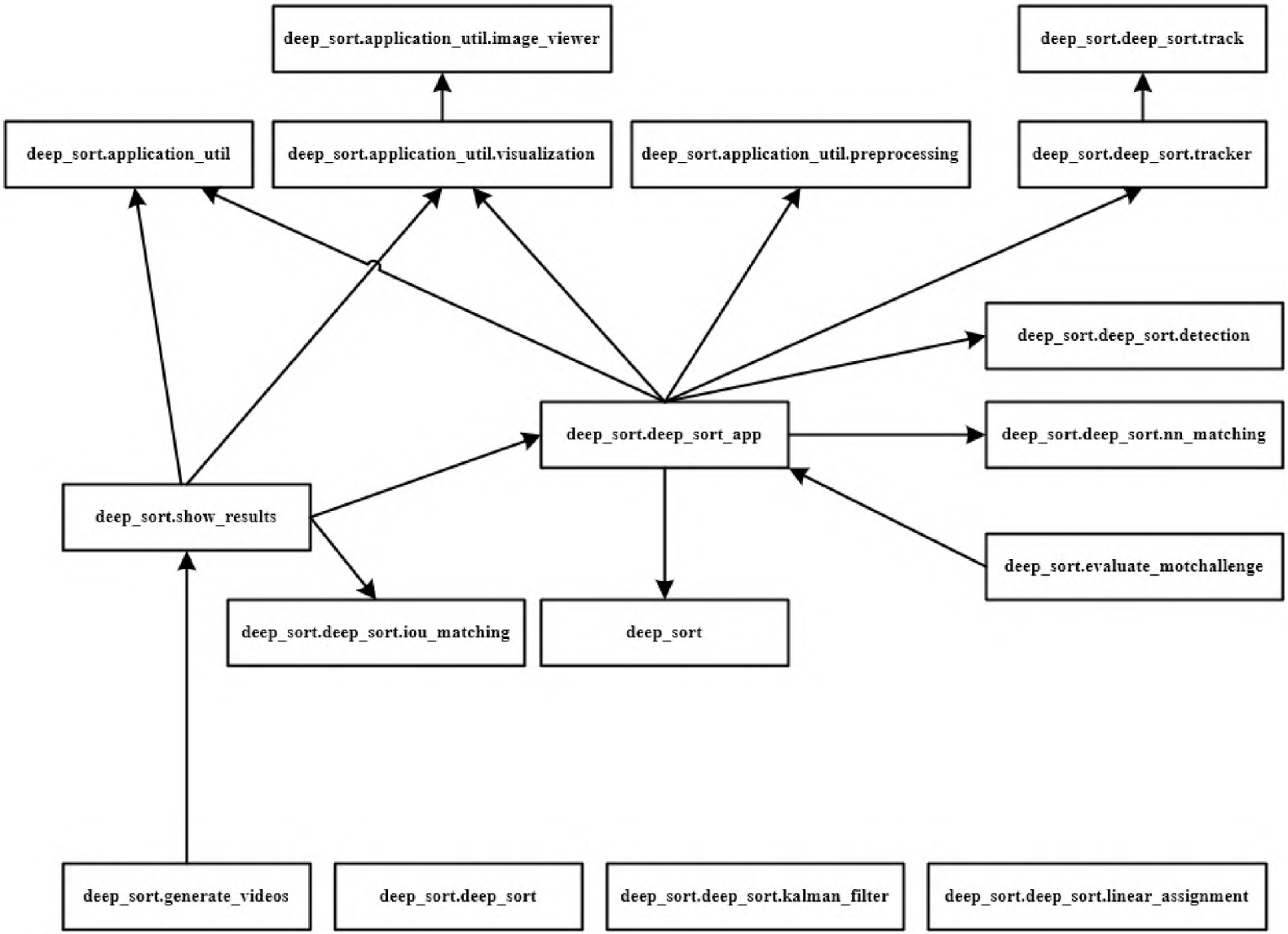


Рисунок 3.7 – Діаграма пакетів системи відслідковування переміщень з використанням алгоритма DeepSort

## 3.3 Функціональні особливості

У процесі детектування існуючих цілей, розміри обмежуючого прямокутника оцінюються за рахунок припущення про його нового положення у наступному кадрі. Матриця призначень вираховується як відстань Жаккара між кожним виявленим та кожним припущеним обмежуючим прямокутником для існуючих цілей. Задача оптимально вирішується за допомогою Угорського алгоритму, що був описаний у розділі 1.5. Більш того, мінімальна відстань Жаккара застосовується для відхилення припущень, де виявлене перекриття менше певного значення. Це використовується для коректної обробки сценаріїв, коли один об'єкт короткочасно перекриває інший. У такому випадку, лише об'єкт, що перекриває, буде відстежуватись, в той час як для перекритого об'єкту не буде робитись припущень.

Коли об'єкт вперше з'являється або остаточно зникає з поля зору, унікальні ідентифікатори відповідно створюються та знищуються. При створенні слідів, будь яке детектування з перекриттям, меншим за мінімальне, сприймається як вірогідна присутність невистеженого об'єкта. Власне слід створюється згідно з розмірами відповідного обмежуючого прямокутника та початковою швидкістю, рівною нулю. Оскільки об'єкт раніше не спостерігався, коваріація його швидкості встановлюється як велике значення, відображаючи таким чином невпевненість. Більш того, нові сліди мають пройти випробний термін, для зменшення кількості похибок першого роду.

Сліди знищуються, коли відповідний об'єкт не спостерігається більше ніж $T$ кадрів. Це запобігає неконтрольований ріст кількості слідів та похибок, пов'язаних з припущеннями про місцезнаходження об'єкта у довгостроковій перспективі без належних виправлень зі сторони детектора. Даний підхід дозволяє калібрувати час $T$, основуючись на особливостях експлуатації, таких як рівень візуального покриття

камерами відеоспостереження, критичність втрати сліду об’єкта спостереження та швидкодія.

### 3.4 Результати роботи програми

Була проведена перевірка швидкодії та ефективності з використанням згенерованого масиву даних. В нього входили відеозаписи, зняті під різним кутом, з різною роздільною здатністю та масштабом. Окрім цього, деякі з відео були записані у русі, що ускладнювало системі роботу. Результат можна бачити на Рисунок 3.8. Алгоритм успішно виявив усіх людей та присвоїв їм унікальні ідентифікатори.


Рисунок 3.8 – Результат роботи програми. Помірна кількість людей, динамічна камера, наявність перекриття

У наборі даних присутні моменти з великими скупченнями людей. І хоча такі ситуації далекі від реальності, коли річ йде про захищений об’єкт, даний уривок

дозволяє перевірити масштабованість системи. На Рисунок 3.9 алгоритм намагається ідентифікувати кожну людину на платформі. Результати задовільні. При цьому швидкодія залишилася на необхідному рівні.


Рисунок 3.9 – Результат роботи програми. Велика кількість людей, динамічна камера, наявність перекриття

Також алгоритм перевірено на даних з вуличної камери, що найбільше схоже по сценарію на спостереження за певним приміщенням (Рисунок 3.10). Алгоритм показав задовільний результат. Варто зауважити, що люди, котрі були лише частково в полі зору камери, не були виявлені, однак це вирішується за рахунок правильного проектування системи відеоспостереження.


Рисунок 3.10 – Результат роботи програми. Статична вулична камера

## 3.5 Аналіз показників роботи алгоритму

Оцінка та порівняння методів багатоцільового відстеження не є тривіальною з багатьох причин. По-перше, на відміну від інших завдань, таких як зменшення рівня шуму у зображенні, у даній області важко досягти ідеального результату. Частково видимі та перекриті цілі, відображення у дзеркальних поверхнях, створюють проблеми для однозначного констатування наявності цілі спостереження. В деяких випадках, при перегляді відеозапису, навіть люди не можуть прийти згоди, а це, в свою чергу, ускладнює можливість створення даних для порівняння. По-друге, кількість різних оціночних показників з вільними параметрами та неоднозначними визначеннями часто призводить до непослідовності кількісних результатів в науковій літературі. Нарешті, відсутність заздалегідь визначених даних тесту та тренувань ускладнює неупереджене порівняння різних методів.

Одночасне відстеження великої цілей є важливою проблемою у задачах опису та розуміння контексту сцени, у якій, на відміну від інших дослідницьких областей, до нещодавна були відсутні бенчмарки та інші методи порівняння показників роботи. З цією метою, був розроблений тест MOTChallenge, що складається з трьох основних компонентів:

1) Публічно доступні набори даних
2) Загальноприйнятий методи оцінки
3) Інфраструктура, що дозволяє додавати нові методи оцінки та набори даних

Результати роботи алгоритму Deep SORT у порівнянні з іншими алгоритмами, представленими на MOT Benchmark, наведені у Таблиця 3.1.

Таблиця 3.1 – Результати роботи алгоритмів у MOT Benchmark

| | *MOTA*↑ | *MOTP*↑ | *MT* ↑ | *ML* ↓ | *ID* ↓ | *FM* ↓ | *FP* ↓ | *FN* ↓ | *Runtime* ↑ |
|---|---|---|---|---|---|---|---|---|---|
| EAMTT | 52.5 | 78.8 | 19.0% | 34.9% | 910 | 1321 | 4407 | 81223 | 12 Hz |
| POI | 66.1 | 79.5 | 34.0% | 20.8% | 805 | 3093 | 5061 | 55914 | 10 Hz |
| SORT | 59.8 | 79.6 | 25.4% | 22.7% | 1423 | 1835 | 8698 | 63245 | 60 Hz |
| Deep SORT | 61.4 | 79.1 | 32.8% | 18.2% | 781 | 2008 | 12852 | 56668 | 40 Hz |

Оцінювання проводиться по наступним критеріям:

- Multi-object tracking accuracy, MOTA (↑): Загальна точність відстеження, що враховує FP, FN, ID
- Multi-object tracking precision, MOTP (↑): Загальна точність визначення положення цілі.

- Mostly tracked, MT (↑): кількість в більшості вистежених траєкторій. Тобто ціль має один і той же ідентифікатор принаймні протягом 80% її тривалості життя.
- Mostly lost, ML (↓) кількість в більшості втрачених траєкторій. Тобто ціль не відслідковується принаймні протягом 20% її тривалості життя.
- Identity switches, ID (↓): кількість разів, коли ідентифікатор об'єкта помилково переходив іншому об'єкту.
- Fragmentation, FM (↓): кількість разів, коли слід було перервано через відсутність виявлення.
- False positive, FP (↓): кількість помилкових виявлень.
- False negative, FN (↓): кількість пропущених виявлень.

Як можна бачити з Таблиця 3.1, алгоритм Deep SORT відповідає сучасним критеріям ефективної системи розпізнавання образів, при чому зберігає можливість його використання у режимі реального часу.

**Висновки до розділу 3**

У ході роботи була спроектована система відслідковування переміщень, з використанням алгоритму Deep SORT. Для цього, мовою UML, були система була описана за допомогою діаграм класів та діаграми пакетів, що відображають логіку роботи та взаємодії компонентів між собою. Спроектована система була реалізована мовою програмування Python з урахуванням специфіки задачі та наявності необхідного інструментарію.

Отримана реалізація системи з використанням алгоритму Deep SORT була перевірено у ряді ситуацій. Навіть при великій кількості об'єктів, що одночасно відстежуються, алгоритм показав задовільну швидкодію і точність. В якості даних

для тестування були вибрані відеозаписи тривалістю від однієї до тридцяти хвилин. У цьому часовому діапазоні програма показала стабільність роботи. Жодних слідів ефектів витоку пам'яті не було виявлено.

В якості об'єктивного показника ефективності алгоритму був вибраний MOT Benchmark, система для тестування алгоритмів з одночасного відслідковування великої кількості об'єктів. Даний бенчмарк насьогодні є єдиною масштабною платформою для тестування та порівняння роботи алгоритмів розпізнавання образів. В даному бенчмарку, використаний алгоритм продемонстрував хороші результати навіть у порівнянні з більш повільними алгоритмами, при цьому зберігаючи частоту обробки кадрів на прийнятному рівні. Найважливішим показником є порівняно низький відсоток втрат слідів об'єктів, що позитивно впливає на якість роботи системи у задачах інформаційної безпеки.

Результатом роботи став програмний продукт, що може бути застосований для описаної у розділі 2 системи. Додавання системи розпізнавання образів не знижує, а навпаки, підвищує рівень захисту інформаційної системи, доповнюючи інші засоби ТЗІ. Точно відслідковуючи положення об'єктів та маючи низький відсоток втрат їх сліду, програма здатна записувати та зберігати ці дані у доступній для подальшого відтворення формі.

# 4 РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

Стартап як форма малого ризикового (венчурного) підприємництва впродовж останнього десятиліття набула широкого розповсюдження у світі через зниження бар'єрів входу в ринок (із появою Інтернету як інструменту комунікацій та збуту стало простіше знаходити споживачів та інвесторів, займатись пошуком ресурсів, перетинати кордони між ринками різних країн), і вважається однією із наріжних складових інноваційної економіки, оскільки за рахунок мобільності, гнучкості та великої кількості стартап-проектів загальна маса інноваційних ідей зростає.

## 4.1 Опис ідеї проекту

Таблиця 4.1 – Опис ідеї стартап-проекту

| *Зміст ідеї* | *Напрямки застосування* | *Вигоди для користувача* |
|---|---|---|
| Програмний продукт, що використовує алгоритми комп'ютерного зору у камерах відеоспостереження та спеціалізується на фізичному захисті інформації на території об'єкту. | Компанії середнього бізнесу інформаційного та інноваційного секторів. | Підвищення рівня захищеності інформації, склад якої містить комерційну таємницю. |
| | Органи державної влади України. | Підвищення рівня захищеності інформації, склад якої містить державну таємницю. |
| | Охоронні агентства. | Можливість використання продукту у пакеті послуг для введення додаткової міри захисту на території об'єкта. |

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

| 1 | 2 | 3 | | | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| № п/п | *Техніко-економічні характеристики ідеї* | *(Потенційні) товари/концепції конкурентів* | | | *W (слабка сторона)* | *N (нейтральна сторона)* | S (сильна сторона) |
| | | Запропонований проект | IntelliVision | iCetana | | | |
| 1. | економічні | Витрати на розробку рішення, отримання ліцензій, сертифікацію, маркетинг та розробку сайту ≈ $60,000 | Витрати на розробку рішення, отримання ліцензій та сертифікацію, маркетинг, розробка сайту, налагодження партнерства та закупка та налаштування обладнання ≈ $100,000 | Витрати на розробку рішення, отримання ліцензій та сертифікацію, маркетинг, розробка сайту, налагодження найм висококваліфікованих співробітників ≈ $120,000 | Менший початковий досвід спеціалістів, недостатні витрати на маркетинг | Регіональна відмінність, оскільки конкурентні рішення в основному представлені на Американському ринку | Відмінність у роді послуг, конкуренти пропонують засоби для забезпечення захисту від підозрілої активності, при цьому не спеціалізуються на розпізнаванні інформаційних загроз |
| 2. | технологічні | Використання алгоритму SORT та його модифікацій | невідомо | невідомо | Можлива початкове відставання у якості програмного продукту | Немає | Використання публічної ліцензії, а отже, відкритий код. |
| 3. | Конфіденційність даних | Забезпечення прозорої політики використання отриманих даних та відкритий код продукту. | Забезпечення прозорої політики використання отриманих даних. | Забезпечення прозорої політики використання отриманих даних. | немає | Немає | Більш високий рівень довіри зі сторони користувачів. |

## 4.2 Технологічний аудит ідеї проекту

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

| № п/п | *Ідея проекту* | *Технології її реалізації* | *Наявність технологій* | *Доступність технологій* |
|---|---|---|---|---|
| 1. | Впровадження програмної реалізації глибокої нейронної мережі, що спеціалізується на відслідковуванні переміщень людей | Використання сучасних наявних трекінгових алгоритмів по типу SORT | Нейронна мережа має бути натренована та розроблений інтерфейс по її управлінню. | Алгоритми знаходяться у вільному доступі, матеріали для тренування можна знайти в мережі або сформувати власноруч. |
| 2. | Технологія довгострокового зберігання даних відеоспостереження, оброблених нейронною мережею для розслідування давніх інцидентів. | Використання спеціального формату обробки та виводу даних мережі, що підходять для зберігання та повторного використання. | Наявні деякі загальноприйняті формати виводу даних нейронної мережі, проте певний документований стандарт не існує. | Технологія є доступною. |
| 3. | Модулі взаємодії з іншими засобами забезпечення фізичної інформаційної безпеки. | Впровадження задокументованого API, що дозволяє використовувати дані обробки зображень з відеокамер іншими програмно-технічними засобами забезпечення інформаційної безпеки. | Співробітництво з виробниками SoC для засобів відеоспостереження, аутентифікації та біометрії. | Співробітництво можливе за умови двосторонньої вигідності партнерства. |
| 4. | Підтримка користувачів та консалтинг з питань контролю доступу та інформаційної безпеки. | Побудова системи для роботи call-центру та відділу з питань підтримки користувачів. | Найм співробітників у відділ з питань підтримки користувачів. | Рішення є доступним. |
| Обрана технологія реалізації ідеї проекту: так як для реалізації ідеї проекту, всі технології є наявними та доступними, тому обираються всі вище описані технології. | | | | |

Таблиця 4.4 – Попередня характеристика потенційного ринку стартап-проекту

| 1 | 2 | 3 |
|---|---|---|
| *№ п/п* | *Показники стану ринку систем відеоспостереження зі штучним інтелектом* | *Характеристика* |
| 1 | Кількість головних гравців, од | Відсутні на вітчизняному ринку, до 20-ти на світовому |
| 2 | Загальний обсяг продаж, грн/ум.од | 20 млн ум.од |
| 3 | Динаміка ринку (якісна оцінка) | Стрімко зростає |
| 4 | Наявність обмежень для входу | Потреба у кадрах із високим рівнем компетентності у сфері інформаційної безпеки та комп'ютерного зору |
| 5 | Специфічні вимоги до стандартизації та сертифікації | Проведення експертиз та сертифікацій щодо стандартизації рішення для використання у державних установах |
| 6 | Середня норма рентабельності в галузі, % | Не менше 175 |

За попередніми оцінками, ринок систем відеоспостереження зі штучним інтелектом є дуже привабливим для входження, але має ряд обмежень та вимог до сертифікації, а також потребує кваліфікованих кадрів.

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

| *№ п/п* | *Потреба, що формує ринок* | *Цільова аудиторія (цільові сегменти ринку)* | *Відмінності у поведінці різних потенційних цільових груп клієнтів* | *Вимоги споживачів до товару* |
|---|---|---|---|---|
| 1 | Покращення рівня захисту, що забезпечують системи відеоспостереження | Компанії середнього бізнесу інформаційного та інноваційного секторів<br>Органи державної влади України<br>Охоронні агентства | Для кожної з трьох категорій існують окремі цінності пропозиції. Пропозиція відрізняється для кожної цільової групи.<br>Надто малий розмір/обмежений бюджет у клієнтів для розгортання повноцінної інфраструктури захисту. | забезпечення надійної та ефективної роботи сервісів, підтримка у режимі 24/7.<br>Сертифікація запропонованого програмного забезпечення, швидке усунення неполадок, проведення консультацій та навчання користувачів. |

Таблиця 4.6 – Фактори загроз

| *№ п/п* | *Фактор* | *Зміст загрози* | *Можливі шляхи реакції компанії* |
|---|---|---|---|
| 1 | Цінова конкуренція | Коливання цін на послуги конкурентів. | Пошук шляхів зниження вартості послуг. |
| 2 | Зниження доходів потенційних споживачів | Зниження купівельної спроможності клієнтів. | Вимушене зменшення обсягів виробництва. |
| 3 | Збільшення розміру податків | Відтік коштів із сфери виробництва до бюджету. | Пошук шляхів мінімізації податків. |
| 4 | Рівень інфляції | Знецінювання коштів, ріст різниці в курсах валют. | Отримання довгострокового кредиту. |

Таблиця 4.7 – Фактори можливостей

| *№ п/п* | *Фактор* | *Зміст можливості* | *Можлива реакція компанії* |
|---|---|---|---|
| 1 | Поява нових технологій та високоефективного обладнання. | Розширення спектру надаваних послуг для клієнтів, збільшення кількості клієнтів, підвищення ефективності роботи продукту. | Впровадження нових технологій для отримання конкурентної переваги, розширення функціоналу, проведення маркетингової компанії. |
| 2 | Стабілізація політичного та економічного становища в державі | Зменшення рівня інфляції, збільшення кількості клієнтів. | Спроби лобіювання інтересів компанії в держаних установах. |
| 3 | Збільшення активності комерційного шпигунства. | Збільшення попиту на послуги систем відеоспостереження. | Залучення нових клієнтів, можливе підвищення вартості послуг. |
| 4 | Залучення нових відомих компаній у якості клієнтів чи постачальників | Збільшення впливу компанії на ринку інформаційної безпеки, зменшення цін на рекламу та маркетинг | Розробка та впровадження нових засобів та програмних комплексів для розширення спектру послуг. |

Таблиця 4.8 – Ступеневий аналіз конкуренції на ринку

| *Особливості конкурентного середовища* | *В чому проявляється дана характеристика* | *Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)* |
|---|---|---|
| Олігополістична конкуренція | Динаміка цін, яка майже не залежить від рівню попиту на продукцію; конкуренція зміщуються в площину реклами, рівня якості продукції та індивідуалізації | Вдосконалення рішення для підвищення якості надаваних послуг для клієнтів |
| За рівнем конкурентної боротьби: національний | Надання послуг для різних груп та типів клієнтів в Україні та за її межами | Застосування новітніх технологій машинного навчання для підвищення конкурентоспроможності. |
| За галузевою ознакою: міжгалузева | Рішення може використовуватися користувачами з різних галузей | Розширення сфери надання послуг, додання нових функцій сервісу та послуг для клієнтів |

Кінець Таблиця 4.8

| *Особливості конкурентного середовища* | *В чому проявляється дана характеристика* | *Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)* |
|---|---|---|
| Конкуренція за видами товарів: товарно-видова | Рішення, що використовується для задоволення потреб клієнтів, але істотно відрізняються від рішень конкурентів. | Надання послуг з підвищення рівня інформаційної безпеки та захищеності території об'єкта, аудиту та консалтингу в сфері інформаційної безпеки |
| За характером конкурентних переваг: цінова | Ціна запропонованого рішення є меншою за рахунок використання вже готових доступних результатів наукових досліджень та розробок. | Надання порівняного рівня послуг, проте з наголосом на інформаційну безпеку та за меншу ціну. |
| За інтенсивністю: марочна | Сукупність характеристик та властивостей рішення | Підвищення якості роботи програмного рішення для клієнтів |

Таблиця 4.9 – Аналіз конкуренції в галузі за М. Портером

| *Складові аналізу* | *Прямі конкуренти в галузі* | *Потенційні конкуренти* | *Постачальники* | *Клієнти* | *Товари замінники* |
|---|---|---|---|---|---|
| | відсутні | iCetana<br>Intelli-vision<br>Darktrace<br>Vintra | Значення розмірів поставок для постачальників. Диференціація витрат | Розміри закупівель державних підприємств та органів влади; рівень чутливості до зміни ціни; контроль якості | Товари замінники відсутні. |
| Висновки | Відсутність жорсткої конкуренції з боку прямих конкурентів. | Є можливості входу на ринок, але існує чимало серйозних конкурентів, що вже працюють на цьому ринку. | Постачальники диктують умови роботи на ринку; компанія, яка здійснює більшу кількість продажів, отримує привілеї та більші розміри знижок на товари та послуги | Клієнти диктують умови на ринку; при організації закупівель товарів та послуг, відчутний рівень відношення до вартості рішення та його якості. | Обмежень на ринку через товари замінники немає. |

Даний проект має принципові можливості для роботи на ринку з огляду на конкурентну ситуацію. Серед сильних сторін, можна виділити використання штучного інтелекту в області відеоспостереження, що не має конкурентних аналогів в Україні. Також, до сильних сторін, порівняно з закордонними конкурентами, можна віднести концентрацію на підвищені рівня інформаційної безпеки та контролю доступу, а не безпеки у сенсі підозрілої поведінки людини у натовпі. Стабілізація політичного та економічного стану, буде сприяти збільшенню рівня попиту на послуги та лобіювання інтересів компанії на рівні держави, а залучення великих відомих компаній в якості постачальників чи клієнтів покращить становище та збільшить вплив на ринку.

Таблиця 4.10 – Обґрунтування факторів конкурентоспроможності

| *№ п/п* | *Фактор конкурентоспроможності* | *Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)* |
|---|---|---|
| 1 | Ціна та змінні витрати | Ціноутворення, яке не є однаковим на послуги для різних типів клієнтів |
| 2 | Розміри закупівель замовників | Розміри закупівель легко масштабуються, оскільки продуктом є програмне рішення |
| 3 | Доступ до ресурсів у конкурентів | Так як потенційні конкуренти вже працюють на ринку, вони мають клієнтів та встановлений шлях продажів та маркетингу, тому вони мають більше ресурсів як матеріальних, так і інформаційних |
| 4 | Гнучкість цін на послуги | Ціноутворення є гнучким, що дозволяє встановлювати її в залежності від клієнту. |
| 5 | Рівень концентрації послуг | Спектр послуг, які можуть бути надані клієнтам є більш вузьким, порівняно з конкурентами. |

Таблиця 4.11 – Порівняльний аналіз сильних та слабких сторін запропонованого рішення

| *№ п/п* | *Фактор конкурентоспроможності* | *Бали 1-20* | *Рейтинг товарів-конкурентів у порівнянні з запропонованим рішенням* | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | -3 | -2 | -1 | 0 | +1 | +2 | +3 |
| 1 | Ціна та змінні витрати | 16 | | | | | | | + |
| 2 | Розміри закупівель замовників | 14 | | + | | | | | |
| 3 | Доступ до ресурсів у конкурентів | 10 | | + | | | | | |
| 4 | Гнучкість цін на послуги | 15 | | | | | | | + |
| 5 | Рівень концентрації послуг | 8 | + | | | | | | |

Таблиця 4.12 – SWOT-аналіз стартап-проекту

| | |
|---|---|
| *Сильні сторони*: використання новітніх технологій, відсутність прямих конкурентів, вузька спеціалізація, можливості гнучкого ціноутворення | *Слабкі сторони*: низький рівень маркетингу, наявність конкуренції у суміжній сфері |
| *Можливості*: швидке впровадження нових технологій; стабілізація політичного та економічного стану, що буде сприяти збільшенню рівня попиту на послуги та лобіювання інтересів компанії на рівні держави; залучення великих відомих компаній в якості постачальників чи клієнтів | *Загрози*: цінова конкуренція; збільшення розміру податків; зниження доходів потенційних споживачів; збільшення рівня інфляції |

Таблиця 4.13 – Вибір цільових груп потенційних споживачів

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| *№ п/п* | *Опис профілю цільової групи потенційних клієнтів* | *Готовність споживачів сприйняти продукт* | *Орієнтовний попит в межах цільової групи (сегменту)* | *Інтенсивність конкуренції в сегменті* | *Простота входу у сегмент* |
| | Компанії середнього бізнесу інформаційного та інноваційного секторів. | Клієнти потребують продукт такого типу та готові ним користуватись | Середній рівень попиту | Існують рішення зі схожим функціоналом, однак які не є замінниками | Є складність входу, пов'язана з високою наукомісткістю виробництва. Необхідна сертифікація товару для успішного входження на ринок. |
| | Органи державної влади України. | Зацікавленість за умови проходження необхідних сертифікацій | Високий рівень попиту, враховуючи відсутність вітчизняних альтернатив | Пряма конкуренція відсутня | |
| | Охоронні агентства. | Клієнти зацікавлені продуктом | Середній рівень попиту | Існують рішення зі схожим функціоналом, однак які не є замінниками | |
| | Поодинокі користувачі (фізичні особи) | Низька зацікавленість | Низький попит, пов'язаний із низьким рівнем загрози витоку інформації, порівняно з вартістю послуг | Пряма конкуренція відсутня | |

На підставі ринкової стратегії обрано використання стратегії диференційованого маркетингу.

Таблиця 4.14 – Визначення базової стратегії розвитку

| *№ п/п* | *Обрана альтернатива розвитку проекту* | *Стратегія охоплення ринку* | *Ключові конкурентоспроможні позиції відповідно до обраної альтернативи* | *Базова стратегія розвитку* |
|---|---|---|---|---|
| 1 | Флангова атака | Стратегія диференційованого маркетингу | Сильні сторони та можливості рішення | Стратегія диференціації |

Таблиця 4.15 – Визначення базової стратегії конкурентної поведінки

| *№ п/п* | *Чи є проект «першопрохідцем» на ринку?* | *Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?* | *Чи буде компанія копіювати основні характеристики товару конкурента, і які?* | *Стратегія конкурентної поведінки* |
|---|---|---|---|---|
| 1 | Частково | Так | Так. Загалом, компанія буде пропонувати системи відеоспостереження зі штучним інтелектом, які вже мають свою нішу. | Стратегія сталого розвитку |

**Висновки до розділу 4**

Результатом проведеного аналізу та оцінки ризиків, було виявлено, що даний проект має можливість для ринкової комерціалізації. До сильних сторін проекту можна віднести майже повну відсутність конкуренції на вітчизняному ринку та наявність молодих конкурентів у суміжній області на світовому ринку. Також перевагою проекту є його наукова місткість та новизна, що може привернути увагу інвесторів. Варто відмітити актуальність теми інформаційної безпеки на державному рівні та тенденції до підвищення норм контролю доступу на територію державних установ.

Для описаного стартап-проекту є гарні перспективи входження в ринок, не зважаючи на наявні певні бар'єри, такі як висока наукоємність галузі та можливість інфляції що може призвести до зменшення ринку послуг.

Отже, можна зробити висновок про доцільність подальшої роботи над імплементацією даного проекту.

# ВИСНОВКИ

Поки штучні нейронні мережі є лише дуже спрощеними аналогами природних нейронних мереж, оскільки нервові системи тварин і людини набагато складніше тих пристроїв, які можна створити за допомогою сучасних технологій. Проте, навіть цього рівня буває достатньо для успішного вирішення багатьох практичних завдань, що підтверджено в ході дослідження.

У розділі 1 були досліджені основні терміни та засади розпізнавання образів. Також були проаналізовані допоміжні алгоритми, такі як фільтр Калмана та Угорський алгоритм, як важливі складові майбутньої системи.

У розділі 2 була проаналізована можливість використання камер відеоспостереження, як самостійного методу захисту інформації. Для перелічених у розділі каналів витоку інформації, насьогодні самостійне застосування алгоритмів комп'ютерного зору в камерах в КСЗІ є недостатньо ефективним по причині відсутності як теоретичної бази з розпізнавання аномальної поведінки в термінах фізичного ЗІ, так і недостатньої потужності обчислювальних засобів.

Незважаючи на це, комп'ютерний зір з успіхом може бути використаний як допоміжний засіб для підвищення рівня захисту ІС. При поєднанні з системою аутентифікації, наприклад, смарт-картами, система відеоспостереження зі штучним інтелектом дозволить відслідковувати переміщення людей, при цьому однозначно ідентифікуючи їх, що відкриває можливості для створення нових правил безпеки а також поліпшує роботу операторів.

У якості основного шляху використання збережених даних про переміщення осіб, було запропоновано побудова теплових карт, що дозволять аргументоване внесення змін у вже існуючу КСЗІ. На основі теплових карт, можна робити висновки про міру ефективності використання інших систем захисту інформації і контролю доступу. Також теплові карти дають можливість до детектування аномальних

переміщень конкретних осіб, тобто може виступати у ролі превентивних засобу з виявлення потенційних загроз.

Запропоновані рішення органічно доповнюють вже існуючі засоби із забезпечення безпеки, в тому числі і інформаційної. Описана система не порушує попередні вимоги до безпеки та конфіденційності даних на різних етапах відеоспостереження.

У 3-му розділі було запропоновано архітектурні та програмно-алгоритмічні рішення щодо системи відеоспостережень, спроектована система відслідковування переміщень з використанням алгоритму Deep SORT. Для цього прототип системи був описаний мовою UML, побудовані діаграми класів та діаграма пакетів, що відображають логіку роботи та взаємодії компонентів між собою. Спроектована система була реалізована мовою програмування Python з урахуванням специфіки задачі та наявності необхідного інструментарію.

Отримана реалізація системи з використанням алгоритму Deep SORT була перевірено у ряді ситуацій. Навіть при великій кількості об'єктів, що одночасно відстежуються, алгоритм показав задовільну швидкодію і точність. В якості даних для тестування були вибрані відеозаписи тривалістю від однієї до тридцяти хвилин. У цьому часовому діапазоні програма показала стабільність роботи.

В якості об'єктивного показника ефективності алгоритму був вибраний MOT Benchmark, система для тестування алгоритмів з одночасного відслідковування великої кількості об'єктів. Даний бенчмарк насьогодні є єдиною масштабною платформою для тестування та порівняння роботи алгоритмів розпізнавання образів. В даному бенчмарку, використаний алгоритм продемонстрував хороші результати навіть у порівнянні з більш повільними алгоритмами, при цьому зберігаючи частоту обробки кадрів на прийнятному рівні. Найважливішим показником є порівняно низький відсоток втрат слідів об'єктів, що позитивно впливає на якість роботи системи у задачах інформаційної безпеки.

Практичним результатом роботи став програмний продукт, що може бути застосований для описаної у розділі 2 системи. Додавання системи розпізнавання образів не знижує, а навпаки, підвищує рівень захисту інформаційної системи, доповнюючи інші засоби ТЗІ. Точно відслідковуючи положення об'єктів та маючи низький відсоток втрат їх сліду, програма здатна записувати та зберігати ці дані у доступній для подальшого відтворення формі.

У ході аналізу та оцінки ризиків проведеного у розділі 4, було виявлено, що даний продукт має можливість для ринкової комерціалізації. До сильних сторін проекту можна віднести майже повну відсутність конкуренції на вітчизняному ринку та наявність молодих конкурентів у суміжній області на світовому ринку. Також перевагою проекту є його наукова місткість та новизна, що може привернути увагу інвесторів.

Отримані результати дозволяють їх подальше використання, як допоміжного методу захисту інформації.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ


1) A. Bewley Simple online and realtime tracking [Text] / A. Bewley, Z Ge, L. Ott, F. Ramos, B. Upcroft // IEEE International Conference on Image Processing (ICIP) – 2016.
2) C. Gao iCAN: Instance-Centric Attention Network for Human-Object Interaction Detection [Text] / C. Gao, Y. Zou, J. Huang // British Machine Vision Conference – 2018
3) D. Stutz Understanding Convolutional Neural Networks [Text] / D. Stutz // Seminar Report, Faculty of Mathematics, Computer Science and Natural Sciences – 2014
4) C. Dicle The way they move: Tracking multiple targets with similar appearance [Text] / C. Dicle, M. Sznaier, O. Camps // International Conference on Computer Vision – 2013
5) L. Leal-Taix´e MOTChallenge 2015: Towards a Benchmark for Multi-Target Tracking [Text] / L. Leal-Taix´e, A. Milan, I. Reid, S. Roth, and K. Schindler // arXiv preprint – 2015.
6) S. Ren Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks [Text] / S. Ren, K. He, R. Girshick, J. Sun // Advances in Neural Information Processing Systems – 2015
7) Вікіпедія, вільна енциклопедія, «Угорський алгоритм» [Електронний ресурс], режим доступу – https://wikipedia.org/wiki/Угорський_алгоритм, 2018
8) T. Lacey Tutorial: the Kalman Filter [Web resource] / T. Lacey // Available at http://web.mit.edu/kirtley/kirtley/binlustuff/literature/control/Kalman%20filter.pdf – 1998
9) F. Yu Poi: Multiple object tracking with high performance detection and appearance feature [Text] / F. Yu, W. Li, Q. Li, Y. Liu, X. Shi, and J. Yan // ECCV. Springer – 2016, pp. 36–42.

10) H. W. Kuhn The Hungarian method for the assignment problem [Web resource] / H. W. Kuhn // Available at http://www.math.harvard.edu/archive/20_spring_05/handouts/assignment_overheads.pdf – 1955.